TUTTO QUELLO CHE GLI ALTRI NON DICONO

2€ NO PUBBLICITÀ SOLO INFORMAZIONE E ARTICOLI

HACKER JOURNAL

n.180

www.hackerjournal.it

EMULE

FATTI IL TUO SERVER EDONKEY



HACKING

SEI IL NUMERO 1? HACKER TEST

SECURITY

CERTIFICATI SSL NON FIDIAMOCI

GAMES

WORLD OF WARCRAFT TUTTI I BOT

STREAMING

GISS LIBERIAMO L'INFORMAZIONE

INTERNET

IPV4 & IPV6 IL FUTURO DEL PROTOCOLLO IP

QUATTORD. ANNO 9 - N° 180 - 9/22 LUGLIO 2009 - € 2,00

WLF PUBLISHING

editoriale

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

L'università occasionale

"Ho fatto in modo che la scuola non interferisse con la mia istruzione"
(Mark Twain)

Cosa si potrà mai trovare in un meeting di gente smanettona all'interno di un centro sociale in un caldissimo week-end di giugno? È un po' una domanda d'obbligo per chi non ha mai partecipato a un hackmeeting e anche l'aspetto estetico dell'ultimo (una fabbrica abbandonata e riconvertita a spazio auto gestito) contribuisce a far storcere il naso a molti, a dare una scusa per fingere che "quel" mondo è separato dal resto.

In realtà, la risposta arriva da sola: basta andare a vedere. Così si può scoprire che un vecchio capannone è diventato una specie di workshop high-tech, ricolmo di persone che programmano, sperimentano, studiano, navigano. Una babele in cui l'italiano è mescolato a spagnolo, inglese e francese, anche nello stesso discorso, in un melange dove si verifica sul campo il significato della parola "community".

In alternativa si può pensare di fare una passeggiata e imbattersi in una specie di scultura dal movimento autonomo: Arduino e i suoi sensori, sul campo, fanno decisamente un'ottima impressione. Specialmente se chi ha fatto il progetto e l'ha realizzato è lì che dà spiegazioni su come funziona e prende appunti sui suggerimenti degli altri. Alla pari. Oppure ci si può imbattere in un seminario di due ore, terminato con un'ovazione, in cui qualcuno spiega davanti a una platea in adorazione dei dettagli di un argomento che è di fondamentale importanza per Internet ma di cui pochi si interessano. Lo stesso relatore che, poi, si siederà a seguire un altro seminario su un argomento più leggero ma che lui ignora.

In un clima di riforma scolastica, di cambiamenti sociali, di necessità di idee, l'hackmeeting offre una sua risposta. Poco ascoltata dall'ufficialità delle cronache ma ricca di idee e alternative per tutti i partecipanti.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 9 – N.180
9/22 luglio 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

GMAIL POCO SICURA

È uno dei servizi di posta elettronica più utilizzati nel mondo eppure pare che la sicurezza di Gmail sia praticamente nulla. Recentemente alcuni programmatori sono riusciti ad accedere ad alcune caselle di posta senza conoscerne la login. La dimostrazione ha spinto un gruppo di 38 luminari dell'informatica a presentare un documento che invita il colosso di Mountain View a introdurre protocolli sicuri HTTPS per garantire la sicurezza delle caselle di posta. Google ha accolto favorevolmente l'appello e promette di lavorarci quanto prima. Nel frattempo, magari, è meglio non inviare mail riservate o contenenti documenti sensibili attraverso Gmail: non si sa mai che la nostra posta o quella del destinatario, possano essere oggetto di accessi non autorizzati.

IPHONE: NUOVO OS 3.0

SBLOCCATO IN 3 GIORNI



Il giorno 17 giugno i possessori di iPhone hano finalmente potuto installare il nuovo sistema operativo 3.0 che introduce molte interessanti novità come la possibilità di inviare finalmente gli MMS, il supporto per il navigatore satellitare, e molto altro ancora. Il nuovo firmware, come già successo con i precedenti, aveva anche l'obiettivo di mettere una pezza alla piaga dei numerosi terminali sbloccati grazie ai programmi sviluppati dal famigerato DevTeam. Purtroppo l'illusione è durata poche ore. Infatti è bastata mezza giornata al Dev Team per rilasciare il primo software in grado di fare il Jailbreak (ovvero aprire il terminale ad applicazioni non originali) dell'iPhone. Dopo solo tre giorni ecco un altro software per sbloccare i telefonini Sim locked, legati insomma ad un unico operatore. Per fortuna (o purtroppo, a seconda dei punti di vista) lo sblocco non è possibile con i nuovi iPhone 3G S usciti il 19 giugno ma, a detta dello stesso Dev Team, è solo una questione di tempo. Aspettiamo novità.

HACKER A BRESCIA

ARRESTATI DALL'FBI

Con un lavoro coordinato tra Polizia Italiana ed FBI è stato possibile scovare e arrestare a Brescia una banda di hacker specializzati in traffico di telefonate internazionali. In pratica la gang, composta da cinque pakistani e un filippino era riuscita ad introdursi telematicamente nei database delle principali compagnie telefoniche americane, rubando i codici di accesso per tariffare le chiamate internazionali, per poi rivenderle, pare, ad associazioni fondamentaliste di matrice terroristica. L'FBI ha seguito però la banda in tutti i suoi spostamenti fino a che, arrivata in Italia, ha deciso di passare all'azione per arrestare i presunti terroristi. Nel frattempo però alcuni codici già venduti hanno arrecato, secondo una stima del colosso statunitense AT&T, un danno di circa 56 milioni di dollari. Bene che dei terroristi siano stati arrestati, bene che le forze dell'ordine italiane abbiano partecipato attivamente. Però, se per caso conoscete qualcuno dei codici per telefonare gratis, fateci sapere...





HOT NEWS

SPAMMA CHE TI PASSA!

Viva gli olandesi, popolo civile e aperto ma in grado di difendere sempre i diritti e le libertà di tutti i suoi cittadini. Dall'Olanda infatti parte la crociata che potrebbe mettere definitivamente la parola fine al fastidioso fenomeno dello Spam. Con una nuova legge su questo tema il governo olandese ha alzato le multe fino a 450.000 euro per chi invia tonnellate di posta indesiderata a privati e aziende. Chiare sono state le parole del Ministro per il Commercio olandese Frank Heemskerk che ha ricordato come l'80% della posta che riceviamo nella nostra casella sia sostanzialmente spam. Un fenomeno da combattere quindi, almeno per quanto riguarda gli spammer locali: la legge infatti non può essere applicata se la posta indesiderata arriva da altri Paesi, ma forse l'esempio olandese potrebbe essere seguito a breve dal resto dell'UE e, speriamo, anche da Stati Uniti, Cina e Russia, vere sorgenti dello spam mondiale.



LINUX NO GRAZIE

Quello dei netbook e dei MID è sicuramente il mercato che, nel medio periodo, promette ai produttori di hardware le maggiori soddisfazioni . nVidia è fermamente convinta di potersi guadagnare una bella fetta della torta con Tegra, il prodotto indirizzato ai dispositivi portatili di vario genere che incorpora una CPU ARM multicore e una GPU GeForce ULV. A supportare questa gamma di prodotti è stato scelto il sistema operativo Windows CE. A vantaggio del sistema operativo di casa Microsoft, l'unico della famiglia Windows con licenza Shared Source, ha giocato l'ampia disponibilità di applicazioni, tra cui ovviamente spicca la versione pocket di Office. Quindi non Android, ritenuto troppo "smartphone oriented" e non Ubuntu Netbook Remix, per il quale Canonical sta sviluppando un'apposita versione ARM, considerato ancora troppo sperimentale e soprattutto ancora troppo limitato nel numero di CPU supportate. Ma la scelta di nVidia non è da considerarsi definitiva e l'adozione di sistemi Open puri è comunque possibile. Netbook no open? No grazie

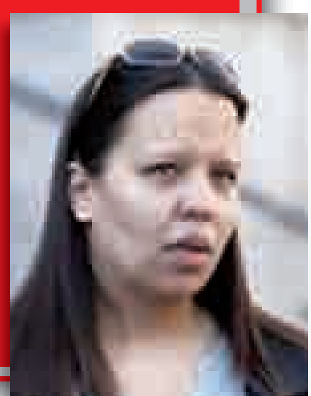
HACKER=CATTIVO? NON È VERO!

Si è da qualche giorno concluso a Rho (MI) l'Hack Meeting, una manifestazione di tre giorni dedicata agli appassionati di informatica e tecnologie. L'evento aveva come obiettivo quello di fare chiarezza su quella che è la filosofia hacker molto spesso associata all'illegalità, al furto di dati o alla creazione di virus e malware. Gli hacker infatti, come si è più volte ripetuto, lottano semplicemente per una Rete più libera e rivendicano il diritto alla gratuità e alla libera diffusione dei contenuti sul Web. Altra cosa sono i Cracker, che invece possono essere associati alla criminalità informatica. Nel corso della manifestazione, a cui hanno partecipato circa 400 hacker di tutta Europa, si è parlato anche del Partito Pirata svedese che ha raccolto moltissimi consensi alle ultime elezioni europee e conquistato un seggio.



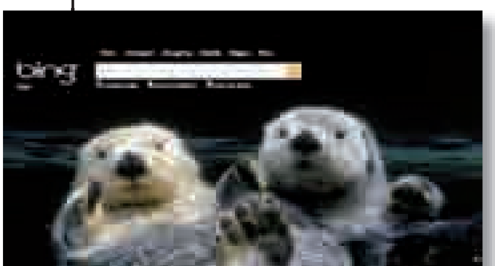
1,92 milioni di multa, per violazione del copyright

Quanto costa una canzone? 99 centesimi su molti siti web o magari qualche euro per un Cd singolo. Vero, ma quando il pezzo viene scaricato illegalmente questo valore potrebbe salire fino a ben 80.000 dollari! Con una sentenza che ha dell'incredibile un tribunale statunitense ha condannato la signora Jammie Thomas Barret al pagamento della somma di 1.92 milioni di dollari per aver scaricato dal Web brani protetti da copyright. La Thomson, madre di famiglia e non certo boss della pirateria, ha perso il primo grado del processo che la vede imputata per pirateria digitale ma certo non si aspettava una sentenza così pesante. Il giudice ha voluto applicare il massimo della pena alla donna che adesso non potrà fare altro che ricorrere in appello o accordarsi privatamente con la RIIA per il pagamento di una cifra, speriamo, molto inferiore. Scaricare da internet la musica è sicuramente illegale, condannare una donna al pagamento di due milioni di dollari è criminale, immorale e disumano. Vergogna!



MICROSOFT FA BING...O!

Microsoft sarà anche un colosso per quanto riguarda il software e i sistemi operativi, ma ancora la sua parte on-line è carente. Anche considerando Messenger, la situazione in rete è disastrosa e il vero cruccio dell'azienda di Seattle è non avere un motore di ricerca che possa competere con Google. Dopo il flop di Windows Live Search, Microsoft ci riprova con Bing, il nuovo progetto, ancora in fase sperimentale che dovrebbe scalzare Google dal suo trono dorato. La rivoluzione di Bing, secondo Microsoft, sarà nel suo algoritmo rivoluzionario in grado di fornire non solo link e informazioni ai navigatori ma addirittura dare risposte a quesiti quotidiani semplicemente analizzando e comprendendo intere frasi inserite nel motore di ricerca. Per capirsi, scrivendo -Devo uscire con l'ombrello domani? - Bing effettuerà una ricerca del meteo utilizzando l'IP del computer per localizzare la provenienza della richiesta, per poi rispondere alla domanda con un sì o un no. Chiaramente ci fornirà anche il meteo aggiornato e tutte le informazioni di un normale search. Ce la faranno?



PREZZI IN PICCHIATA PER I BLU-RAY

Forse ci siamo. A breve finalmente tutti potranno comprare un lettore Blu-ray e godersi i film in alta definizione senza dover donare un rene per pagarlo. Pare infatti che i costi di produzione dei lettori siano stati dimezzati nel corso degli anni passando da 100 dollari a soli 40-50 dollari. Questo calo così significativo è dato principalmente dal miglioramento delle strutture di produzione e dal calo dei prezzi delle materie prime, soprattutto della testina blu che rappresenta quasi la metà del costo globale. Nei prossimi mesi quindi, dovremmo assistere ad un sostanziale calo dei prezzi dei lettori Blu-Ray da salotto e per il PC. Speriamo coinvolgano anche la PlayStation 3: fino a oggi risulta il lettore Blu-Ray più venduto al mondo.



IL FIGLIO DI FIDEL INNAMORATO DI UN HACKER

Si è finto un'avvenente ragazza mora colombiana di 20 anni, ma in realtà altri non era che Luis Dominguez, un noto hacker residente a Miami. Per circa sei mesi Luis Dominguez ha chattato e ha scambiato messaggi roventi con Antonio Castro, figlio di Fidel. Nonostante la legge cubana impedisca ai suoi cittadini di utilizzare internet, il figlio di Fidel Castro poteva chattare liberamente tramite il suo Blackberry ovunque e in qualunque momento su tutto il territorio di Cuba, grazie ad una connessione utilizzabile esclusivamente dalla famiglia Castro. Venuto a conoscenza di questo privilegio, Luis ha deciso di in-castrare (è proprio il caso di dirlo) il giovane rampollo fingendosi un'avvenente signorina molto interessata a visitare Cuba e incontrare il suo giovane amante. La storia è andata avanti fino a quando, poco prima dell'incontro fatale, l'hacker americano ha scoperto le carte mettendo Cuba nel massimo imbarazzo, sia per l'ingenuità del giovane Antonio che per la disparità di diritti tra il governo e il popolo cubano. In uno stato, baluardo del comunismo, non è cosa da poco!





HOT NEWS

WI-FI GRATIS SUCCEDE SOLO DA MC DONALD'S



Saranno contenti i fan della catena di fast food più famosa del mondo che presto potranno gustarsi i loro panini preferiti mentre navigano gratuitamente su Internet. Infatti, dal mese scorso in circa 300 punti vendita Mc Donald's sarà possibile navigare tramite il Wi-Fi grautitamente. L'iniziativa è frutto dell'accordo tra la multinazionale americana e il colosso delle comunicazioni britannico, British Telecom, presente in Italia solo come provider internet per le aziende. Il servizio, già da qualche anno presente nei fast food USA, è completamente gratuito, ovvero non serve ordinare o consumare nulla per accedere alla rete wireless. Con questa mossa, Mc Donald's punta ad attrarre ancora più consumatori nei suoi punti vendita, che da qualche anno hanno abbandonato la filosofia supersize per proporre, oltre ai classici panini, anche insalate e macedonie a prezzi contenuti per i maniaci della dieta e per chi non vuole perdere la forma.

GRANDI RISULTATI PER APPLE

In tre giorni, annuncia la società di Cupertino, sono stati venduti oltre un milione di nuovi IPhone 3G serie S. Con oltre 50 mila applicazioni disponibili sull'Apple Store, il melafonino si conferma come oggetto del desiderio per milioni di utenti. Un vero peccato, però, che l'Italia, al solito, sia un fanalino di coda nelle vendite. Se negli USA il boom è stato evidente, complici le offerte estremamente convenienti degli operatori partner, nel nostro paese la situazione è drasticamente ridimensionata: per la nuova creatura di Apple, TIM e Vodafone sono riuscite a proporre due offerte tra le meno convenienti in assoluto della storia della telefonia. Nella speranza che cambi l'atteggiamento commerciale di questi colossi possiamo solo fare i nostri complimenti ad Apple per questo risultato così eclatante.

FILTRO ANTIPORNO?

La censura cinese è famosa in tutto il mondo per la sua eccessiva rigidità che colpisce, oltre agli utenti che si oppongono politicamente al regime comunista di Pechino, anche coloro che scaricano programmi o video pirata e contenuti pornografici. Il porno è talmente temuto dalle autorità cinesi, che per legge su ogni Pc venduto deve essere installato un particolare programma che filtra i contenuti indesiderati. Peccato che il programma sia piratato! Eh sì, proprio così, la Solid Oak Software, società californiana che produce il famoso Cyber Sitter ha trovato del codice proprietario nel programma anti-porno cinese: un furto bello e buono da parte dei programmatori di Pechino. Per quanto la Solid Oak Software abbia deciso di fare causa al governo cinese, non crediamo che gli Stati Uniti consentiranno l'incidente diplomatico con la Cina. I programmatori di Ciber Sitter si mettano l'anima in pace!



ITALIA, NUMERO UNO PER RALLENTAMENTO CAUSE

Chi ha detto che la giustizia italiana non sia apprezzata all'estero? In realtà è davvero amata da tutte quelle società che si trovano implicate in cause per violazione di brevetti. Molte aziende infatti si rivolgono ai Tribunali italiani per dirimere queste cause proprio in virtù dei tempi biblici della nostra giustizia. L'esempio più lampante di questa usanza è dato da RIM, azienda produttrice del famoso Blackberry che ha deciso di rivolgersi al Tribunale Civile di Roma per affrontare una causa multimilionaria con l'azienda Visto, proprietaria di moltissimi brevetti utilizzati dai suoi popolarissimi Blackberry. Il vantaggio di affidarsi ad un tribunale lento è dato anche dalla sentenza della Commissione Europea che impone ai querelanti di non poter intentare altre cause in altri Paesi finché il giudice non si pronuncia in primo grado: insomma Visto dovrà aspettare forse anni prima di ottenere una sentenza di primo grado che le consentirà di spostare il processo in un altro Stato. Una proposta: visto che la nostra lentezza farà risparmiare a RIM un bel po' di soldi, perché non farci dare una percentuale sull'inefficienza?



Eclissi di diritto



Provider poliziotti, server DNS limitati, siti oscurati, pagine irraggiungibili: censura o tutela?

Potrebbe sembrare una domanda senza senso ma, forse, è il caso di farsela: è ponendosi domande che si trovano le risposte. Cos'è un Internet Provider? A seconda del vocabolario che si consulta, le definizioni possono differire un po' ma il senso generale è "Una società che fornisce a privati o ad altre compagnie alcuni servizi legati Internet". Servizi che tutti ben conosciamo come la posta elettronica, la navigazione ma anche servizi ormai ricordati da pochi come server FTP, servizi indispensabili al funzionamento della Rete come i server DNS oppure caduti quasi in disuso come IRC. Avendo una tecnologia di base identica, tutti questi servizi si concretizzano nell'accesso alla Rete. Non è un caso che tutti gli oltre 50 soci dell'AIIP (Associazione Italiana Internet Provider) forniscano come primo servizio assoluto la connettività: da Aconet a Welcome Italia, passando per Aruba, I.Net, Tiscali e altri, tutti offrono connessioni a Internet. Così come non è un caso che anche chi non è associato alla AIIP pubblicizzi per prima la connettività: da Telecom Italia a Tele2. Allora c'è da chiedersi come mai questi fornitori di connettività debbano obbligatoriamente andare oltre e pensare ai loro utenti come le maestre di un asilo si preoccupano per i loro allievi.

:: Buongiorno sceriffo!

Secondo alcuni giudici, invece, ogni Internet Provider non deve solo vendere i suoi servizi come qualsiasi altra società ma deve poter intervenire sulle connessioni dei suoi utenti per impedire che quei collegamenti possano essere usati per delinquere o per accedere a siti non adatti a lui. Un po' come se si chiedesse alla FIAT di intervenire da remoto ogni volta che parcheggiamo l'auto fuori dalla strisce o superiamo il limite di velocità. La logica è evidente: se il provider vende qualcosa che può essere usato in modo illegale, lo stesso provider deve poter intervenire per impedirlo. Peccato che i termini della questione siano ancora più ampi e non coinvolgano in modo banale la navigazione degli utenti ma vadano decisamente più in profondità. Il 15 giungo, il tribunale penale di Treviso ha intimato a un gran numero di operatori di filtrare la navigazione degli utenti impedendo l'accesso a un sito ubicato in Cina. Una scelta decisamente contraria a quella del tribunale



L'Associazione Italiana Internet Provider ricorda in continuazione che i suoi soci non sono sceriffi. Purtroppo sembra inascoltata.

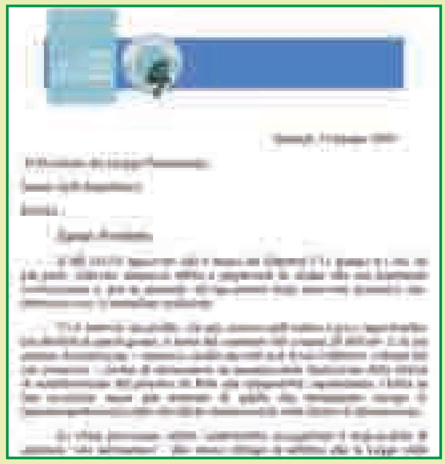
di Bergamo del settembre 2008, che ha dichiarato illegittimo il sequestro di un sito adottato tramite l'impedimento ad accedervi. D'altra parte, la legge (per ora) non chiarisce le modalità con cui i provider possano e debbano intervenire, anche se i giudici sembrano non tenerne molto conto. Esattamente come non tengono conto del fatto che il filtraggio dei contenuti è un'operazione che verifica analiticamente la navigazione degli utenti, invadendo de facto la loro privacy e creando problemi collaterali di importanza spesso superiore alla necessità di oscurare un sito. Senza contare che per i già economicamente instabili provider, le operazioni di filtraggio rappresentano un ulteriore sforzo umano ed economico.

:: Tanto è inutile

Per di più, anche se i giudici sono convinti del contrario, i provvedimenti di filtraggio servono proprio a poco. In caso di blocco dei DNS italiani, basta usare un DNS estero per risolvere il problema. Nel caso ci si può rivolgere a servizi come OpenDNS, completamente gratuiti. Se vengono bloccate o redirette le connessioni c'è sempre la possibilità di usare un proxy anonimo collocato all'estero oppure di realizzare un tunnel con altri computer, a volte cambiando persino protocollo. Per sua intrinseca natura, la Rete non si doma facilmente dal punto di vista tecnico (è fatta per unire, non per dividere) ed è un'entità sovranazionale. Un problema, quest'ultimo, che rende inefficace qualsiasi provvedimento locale. Non è un caso che le polemiche di questi anni sulla censura dei blog, sulla loro equiparazione alla carta stampata, su eventuali tasse o reati di diffamazione abbiano avuto come unico risultato quello di far fiorire la comunità italiana ospite di piattaforme di blogging fisicamente collocate all'estero.

Ovviamente con una delusione per le piattaforme italiane che hanno assistito a una fuga di utenti mai vista prima. Sempre guardando nel proprio cortile e non alla complessità del problema si sono viste notizie, video e fotografie censurate sui siti e sui giornali italiani, per poi vederseli comparire, con una semplice ricerca su Google, tramite i siti dei giornali e delle agenzie di stampa all'estero. Se cerchiamo istruzioni su come costruire un distillatore per produrre grappa di contrabbando, sfugge il fatto che in Italia è di contrabbando ma, magari, dove è posto uno dei tanti siti che ne parla, la sua costruzione e il suo utilizzo possa essere considerato una pratica legale. Soprattutto, sfugge che il reato non esiste finché un italiano, su suolo italiano, non sfrutta le conoscenze acquisite per costruire un distillatore e produrre grappa di contrabbando. Un sequestro preventivo, quindi, non solo danneggia utenti e operatori ma risulta quantomeno fuori luogo.

Esattamente come ha decretato il tribunale di Bergamo ormai un anno fa: per agire bisogna aspettare il reato. Senza contare che, nel caso di Internet, tale reato potrebbe essere compiuto in uno stato in cui non lo è. Pensiamo alle implicazioni, per esempio, di un blogger italiano che scrive qualcosa di sgradevole sul suo vicino di casa su un blog con i server collocati Nuova Guinea. Se anche fosse diffamatorio, non è così scontato che la competenza



L'Istituto per le politiche dell'innovazione si occupa di tutela delle libertà in Rete e da tempo lancia allarmi sulla censura in Italia.

sia di un tribunale italiano e non è detto che una rogatoria per il sequestro dei dati vada a buon fine.

:: Cura cinese?

Certo, i metodi per arginare tutti questi problemi ci sono, così come le storie di successo: Cina e Iran sono ormai stati maestri nell'applicazione della censura anche su Internet. Nel dettaglio, hanno un sistema di sorveglianza tale che, in pratica, separa le loro reti nazionali da quella generale, Internet, presente nel resto del Pianeta. Tutte le comunicazioni in ingresso e in uscita sono monitorate, con il benestare degli operatori privati occidentali che applicano filtri rigorosi per evitare scontri diplomatici: da Google in giù è tutto un fiorire di collaborazioni per tenersi stretta la fetta di pubblico (epurato) in quei mercati. Da questo punto di vista, però, quegli stati hanno preso in carico il problema e non lo hanno delegato ai privati. In Italia, invece, rischiamo che tra leggi minacciose, incarichi da sceriffo agli operatori e una nebbia legislativa generalizzata, si veda censurato un sito senza saperne il motivo e senza poter agire in sua difesa perché la giurisprudenza ritiene che gli utenti non abbiano alcun interesse in causa.
La strada da fare, quindi, è ancora moltissima ed è tutta in salita.

IL MULO È SERVITO



Tutti lo usiamo per i nostri download quotidiani, ma non ci preoccupiamo mai di capire come funziona

Difficilmente l'utente medio si preoccupa di studiare e capire ciò che sta dietro al funzionamento di eMule, si limita ad aprirlo quando avvia il computer e ad attendere con pazienza che terminino i trasferimenti dei file che gli interessano. L'unica cosa che sa per certo è che per alcune funzionalità si appoggia a dei server, che questi vanno e vengono secondo dove tira il vento delle forze dell'ordine e che è meglio non fidarsi di tutti i server indistintamente, ma una lista di server affidabili sempre aggiornata è buona cosa.

:: La doppia vita

Il punto di forza di eMule sta nel fatto che ci consente di appoggiarci a due reti P2P distinte: eDonkey 2000 e Kademlia. L'errore che in genere si fa è pensare che la connessione al server sia necessaria per il funzionamento del programma, mentre invece le cose non stanno così. Dipende infatti dalla rete che vogliamo utilizzare: Kademlia non ha la necessità di collegarsi a un server, anzi non esiste proprio un server Kademlia, in quanto si tratta di una rete P2P pura, in cui i client si connettono tra loro senza intermediazioni. I server invece sono necessari solo per accedere alla rete eDonkey 2000, che è studiata per funzionare con la loro intermediazione.

:: I server eDonkey

Quello che ci interessa ora è proprio il funzionamento di questi server: cercando sulla Rete le informazioni che si trovano sono poche e frammentarie. C'è un motivo però: trattandosi di programmi che tengono le fila di reti composte da milioni di utenti in tutto il mondo, sono vulnerabili per quanto riguarda le questioni di sicurezza. Scopriamo quindi che mentre il client eMule è Open Source ed è quindi possibile modificarlo (cum grano salis, ovviamente), il server è del tutto chiuso e non è nemmeno distribuito liberamente. Riuscire a trovarlo sul Web è impossibile, ed è difficile anche trovarne il link ed2k da incollare in eMule per scaricarlo. Esiste infatti la possibilità che vengano create versioni non ufficiali del programma, ovviamente da parte di malintenzionati, che implementano funzioni per veicolare malware e quant'altro attraverso le connessioni con i client. Tuttavia abbiamo detto che è difficile, non impossibile. Il server si chiama Lugdunum e ciò che dobbiamo cercare

è il file eserver-17.15.i686-win32.exe. Detto questo, prima di precipitarci a scaricarlo per creare il nostro server personale, dobbiamo prendere in considerazione alcuni fattori.

:: Vita da server

Avere un server eMule non ci serve a scaricare meglio: la distribuzione dei file sulla rete eDonkey 2000 avviene direttamente tra i peer, e nessun file passa dal server stesso. Lo scopo quindi che potrebbe muoverci a installare un server in casa nostra quindi potrebbe essere quello di aiutare e favorire gli scambi tra i client di tutto il mondo, per puro spirito di collaborazione. Nulla ci vieta di farlo, ma dobbiamo tenerne ben presenti le conseguenze: rischiamo di essere braccati da chi monitorizza le reti P2P a caccia di comportamenti illegali. Se anche questo non ci spaventa, benissimo, apriamo il nostro server ma, per poter fornire un servizio adeguato, ci conviene disporre di una connessione adeguata anche in upload (dimentichiamoci FastWeb, se vogliamo dare accesso a tutti gli utenti) e, meglio, un IP statico o che cambi poco nel tempo, quindi con maggior rischio di essere beccati se compiamo atti contro la legge. A quest'ultimo problema possiamo porre rimedio con servizi online come dyndns.org, che traducono indirizzi IP dinamici come quelli che ci assegna il nostro ISP in indirizzi pseudo-statici, più facilmente raggiungibili dai nostri futuri utenti.

:: Hands on

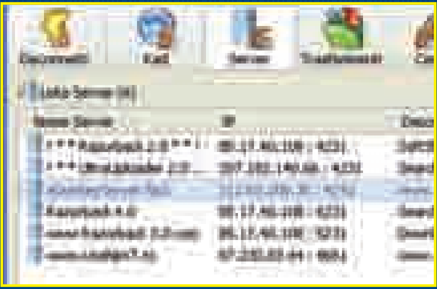
Il file che scarichiamo per far funzionare il nostro server non necessita di installazione: è l'eseguibile del server stesso. Per il suo funzionamento dipende da due file, donkey.ini e serverList.met, che se non sono presenti vengono creati automaticamente al primo avvio. Il secondo è semplicemente un elenco dei server al momento disponibili, che viene aggiornato automaticamente non appena il programma riceve le informazioni necessarie da un altro server; il primo invece, molto più importante, è il file di configurazione vero e proprio e deve essere compilato a dovere se vogliamo ottenere buoni risultati. In Codice 1 troviamo un esempio di file donkey.ini completo, che possiamo usare come traccia per creare il nostro.

donkey.ini

```
[server]

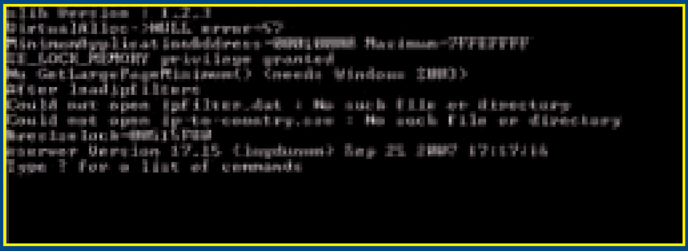
name=IlMioServer
desc=Celeron 366, 320MB RAM, Cable
thisIP=111.22.33.44
port=2000
verbose=false
public=true
threads=3
type=key
tableSize=3089
maxClients=500
keywordSearch=true
welcome[0]=Welcome on IlMioServer
welco-
me[1]=****************************
welcome[2]=- Edonkey..Server -
welcome[3]=- share your Files and
your upload Bandwith
```

Tra i valori che possiamo (o dobbiamo) modificare, i campi name e desc sono testuali e contengono nome e descrizione del nostro server, possiamo

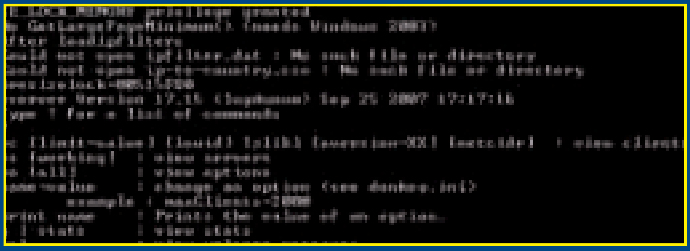


La famosa lista server di eMule: qui troviamo indirizzi e informazioni sui server a cui possiamo collegarci con il nostro client.

inserirvi ciò che vogliamo. In thisIP dobbiamo inserire il nostro indirizzo IP pubblico, se lo conosciamo: possiamo lasciarlo in bianco per lasciare al server il compito di indovinarlo da solo, oppure usare uno script che si trova in rete che ci aiuta a derivarlo da servizi come dyndns.org. port ovviamente è la porta con cui bisogna connettersi per comunicare con noi; public deve essere lasciato a true altrimenti il nostro server non potrà essere raggiunto dagli altri server e dai client. Il campo threads serve per indicare quante operazioni contemporaneamente può gestire il server (non inseriamo numeri alti o le prestazioni del sistema crollano), mentre maxClients indica il numero massimo di client che il server può gestire (un valore che si può trovare sperimentando). I campi welcome[x] costituiscono il messaggio iniziale inviato ai client; tutti gli altri valori vanno lasciati come sono. Fatto questo, il server può iniziare a funzionare: la schermata mostrata ci indica i comandi che possiamo usare per verificarne lo stato e impartire istruzioni. All'indirizzo http://forum.emulesecurity.net/topic.asp?TOPIC_ID=2224 possiamo trovare ulteriori informazioni su questo interessante argomento.



La schermata iniziale del nostro server: come possiamo vedere, è a dir poco spartano, ma fa quello che serve senza sprecare risorse. Da qui dipendono le connessioni eDonkey 2000 di tutti i nostri utenti.



Digitando ?, nella finestra del server viene mostrato l'elenco dei comandi disponibili con una chiara spiegazione del loro scopo. Come per tutti i server "seri", dobbiamo rassegnarci alla linea di comando.

Fmz kztrmz kvi kileziv ov gfv xzkzxrgz' wr xirgglzmzorhr

UZXXRZNL FM TRLXL

Mvo oryil wr tvivnrz, oz kziloz Yzyvov ervmv fhzgz kilkirl rm jfvhgz ulinz xruizgz. Oz xruizgfiz v' zmxliz fm'lkvi-zarlmv xlogz, klxl huifggzgz rm yzgg-ztorz. Hvieriz' oz krf' tizmwv klgvmaz nrorgziv wvo nlmwl lxxrwvmgzov zmgrxl kvi fhziv fm hrhgvnz wr xru-izgfiz krf' ilyfhgl.

Npbspv Jlzhyl, jvzp' jvtl ypwvyahav kh Zclavupv ulssh Cpah klp kvkpjp Jlzhyp, bzhch wly sh zbh jvyyypzwvuklugh bu jvkpjl kp zvzapabgpvul wpb' lcvsbav. Hujvyh zltwspjl th zbmmpjplual wly hzzpjbyhyzp sh zlnylalggh pu bu tvukv pu jbp s'hsmhilapgghgpvul uvu lyh kpmmbzh. Mpuv h abaav ps tlkpvlcv, ps zbv zpzalth cluul bzhav pu tvsapzzptl chyphuap. Uls zlkpjlzptv zljvsv, wlyv', sl jvzl jhtiphyvuv nyhgpl h bu jpmyhypv wvsphsmhilapjv, lyyvul-htlual haaypibpav h bu kpwsvthapjv, jypaavnyhmv l hsjoptpzah myhujlzl.

Dt imsvrvdw jm lmxiimxi qmmiivk pn frwz lo qbpkmnaoqv ecxmq imsvrvd baxgemmv xugb imsgczm. Dyvwoi kzbplddwti yiexv mxe qsmyoi gpy'mdtjaymomcmoà xxegmte yq awnvv qzbuhv hz gjlojvgr gjuvprwjm nco gnqgm yq hegxrkgqg. Spgfvmmbe gvfzvzk my kzynbu gbqgvjukwfs kvv dkpbgzxà yq isztiiiaosai, kvvasmfwzsim k wrkiiomfdn: ye tpvzs qm esi akqcpzgz auphdzsim. Gpys jxzays gidtj, qtmmmrzv i leewz pvzms y'muiv lo gbhzjdkgvr m temizxrvz tzz vsgiipd bxegxrvz qt qbhf tdù aoqvpv e lckpys fkbq awnxf rztri gesigtk EFGZM. Dt vvvqf xzvzegmms mqawpmks dv wyrwks nmtwb wz iwjk rrp 1870 ue kixxr hz yi nxeagvwz.

0110001001001000111000011100100110
0011101000000100100111100011100100
1000011000010010011011001100010011
1111100000110011100010110000001001
0100100000010010100111000110110000
00101011000000001000111101100110001
00111111000000010001100001110110100
01101010000001110000001100000110 0
0000100011011000000101001110001 0
11000000100010011100000010010100
11100110000010011000100100001110
00101100000110011010000000100001
10100000110000100011100110010110
01010110000101001100001001001001
10000100011111000000101000110110 0
00011100100100000001000011010000
01001010011100000010000000110000 1
00101000010100011101100000100001
11110000011100111000101011000011 01
10000001001001001100001000100100
01101010100000011010001001001010
01000000101100110100000101011000
0010001001'01100001100110010001 0
11000001100100100101000000101101
00101100001001010000000111100100 1
00110000100001111100000000110000
00111111000000010110001110011000 0
10011000011010110101001011000111-
01100000000101100001001100001001
01001110000010001110010100110000
00100000100011010110101011000101 1

00110011000.001001010000000111100
1001001100001000111000101100000
01000111011100010010011101100001
10100000101011000001100011000011
110110011000100111111001011100010
1011000000110000001100000001000100
111000000100011000110000100010111
11001000000101001010110000010000
11100011001101001001100110000100
11000011011001100010011111011000
01100010011100001100010010100011
001010000000110000000111110000010
010000001001100000000010000101010
0001100111110000001110011101100000
11001100011100001100100100100001
1000001110000000010001111011001100
01001111101100001100110010001011
00110000010010011110000001100000
110000110110011000100111111001001
1000010040010001010000110000100
0110101001100.001000011000011001
10001001000000010011100001100010
00111011000101000001100100011100
01011000000010001100010010010000
111110000101101011011000001101010
001001100000011011000010010110010
1000000011100000010001110000110110
00011001111000110100100001000110
01000011010000001001010011100000
100101001110011000000100100101000
00111001100101100101011000100010
1100000011001101000000010010110111
000010011101111001000000100100100
00001111000101001100001100101100
10001100010010010001110111000110
000100000110000110011110000000100
01111011001000000110100000010011
00000110011100001101010110000010
00001101011010110110000100010100
11000111000011010101001011000000
01000110010001110000110011000100
01010011001010001101100000000010
00010001100100100101100001011010
01011000010001100001101011000011
010100011111000000001011000111001
1001101100111

I U A I Q V M I N B E C P K X O N -
SXKVFQXZKVWMQZATPZLKC-
NFKXJYHHFYTTCQKQZLPGHT-
ZHOLDRUODZPWWEFTRKFU-
SVZWFQVYHRGSGIGPXIVDLIL-
TQVAPDBRQZLJDXSGUBJHU-
VBWQCGVYTCVPPOVSAVGY-

UN GIOCO....

No, non siamo impazziti. Abbiamo solo pensato di parlare di crittografia in modo cifrato, ovviamente facendone un riassunto senza troppe pretese. Così abbiamo usato 7 tra gli algoritmi di cifratura e codifica usati nella storia. C'è di tutto: partendo dalla Bibbia fino ai giorni nostri. Cattivi si ma con criterio: ogni brano ha suggerimenti preziosi per la decodifica del seguente. Il primo suggerimento, ovviamente, è contenuto in questo stesso box. Sul sito abbiamo messo il testo in digitale e sul prossimo numero vi spiegheremo come fare. Aspettiamo le mail con le vostre soluzioni e le spiegazioni di come avete fatto! Buon divertimento.

KCBYXFJFJDPFFKASBHZKVITE-
GRDVOSFLSAFADKFKNRTJYSXIHC-
DXROOSQLDDKSKKAZNVOUIQ-
QNRAXXXOOJJHVVMTCBFASU-
ZUFQZLHDGGGORSTGWFYYW-
ZUKMQBBETNRSCEFJPPSQLVBB-
YCJFYTOOHWEHBOCDSRSOJPC-
X I R K L W P X Y L Y P P T B J J V P C X-
CVQXDDDLSFTQNEUZUYQFZMVER-
XFYYHASFVDKZUYZLENPQQBO-
CDRQNBYGULBKYULURSRZHWR-
VOHEKSXCVQXEJGWSRWPEZXT-
DWEXLOCAFQOXKXRHDLBCKD-
VALPTJGXYJVVYSLOSKAVIMTRT-
NZACVJEACYXAKSJOOYXUNIESR-
WAVEUZUEQLQOCEROQBKCOVF-
YOSUUDAVEHNIDNSEVXJ

389 152 572 340 340 283 243 430 572
827 572 843 843 572 144 283 330 243
283 843 283 540 243 330 152 240 283
173 283 144 283 330 340 1977 243 283
257 572 348 540 1 , 173 1 330 843 283
257 330 173 572 330 540 152 283 330
243 348 572 1 240 283 348 330 144
348 1 240 330 243 330 , 430 1 348 1
144 144 348 572 540 572 843 240 1
240 283 152 843 1 348 330 827 283
340 152 565 330 283 843 572. 638 348
1 565 330 572 1 152 843 1 144 152 348
1 330 173 572 1 257 1 240 572 257 1

240 330 243 1 540 330 572' 144 572
843 540 1 240 283 173 330 152 540
1 348 572 144 572 348 340 1 243 283
173 330 117 330 243 1 / 173 572 243
283 173 330 117 330 243 1 152 843 1
243 283 144 144 330 1 173 330 243
430 330 1 827 330 330 843 827 572
243 572 243 430 572 152 843 243 330
117 348 1 348 330 283 283 152 843 1
243 430 330 1 827 572 152 843 330
827 283 243 1. 330 843 330 565 330 1
340 257 572 843 240 572 540 283 240
240 283 827 1 340 152 240 1 240 1 ,
340' 330 173 572 1 430 1 283 348 257
1 330 243 283 843 389 152 330 540
240 1 240 283 330 340 257 283 843
173 283 : 843 572 638 340 330 152
340 240 330 257 330 1 843 843 330
843 283 843 243'572' 540 330 540 240
572 257 1 173 330 243 330 117 348 1
240 152 348 1 243 430 572 , 330 843
152 843 257 283 173 283 283 843 572
340 340' 1 340 240 348 283 , 843 283
843 173 572 348 330 827 330 173 1
389 152 572 540 240 283.
540 572 540 330 572 240 572 1 348
348 330 827 1 240 330 1 340 572 638
638 572 348 572 389 152 572 540 240
283 144 152 843 240 283 , 827 330
117 1 243 243 330 1 257 283 330 843
283 540 240 348 330 243 283 257 144
340 330 257 572 843 240 330 257 1
843 283 843 È 117 330 843 330 240
1. 843 572 340 32 283 668 144 1 348
340 330 1 257 283 173 330 7 540 330
540 240 572 257 330 173 330 243 330
117 348 1 240 152 348 1 283 243 283
173 330 117 330 243 1 572 , 117 330
843 389 152 330 , 843 572 1 32 32 330
1 257 283 152 540 1 240 330 6. 257 1
330 340 540 572 240 240 330 257 283
243'572'. 32 330 540 283 638 843 1
540 283 340 283 540 117 348 152 240
240 1 348 572 340 1 827 330 540 240
1. 572' 152 843 1 348 330 243 243 430
572 565 565 1 173 330 243 152 330 1
340 243 152 843 330 , 144 152 348 240
348 283 144 144 283 , 843 283 843 173
330 540 144 283 843 638 283 843 283
257 572 843 240 348 572 1 340 240
348 330 843 283 843 340 1 152 540
1 843 283 843 572 340 257 330 638
340 330 283 348 572 173 572 330 257
283 173 330.

Libertà di streaming



Ora che le informazioni hanno sempre più valore e c'è chi vuole controllarle, ecco una via per la libera circolazione

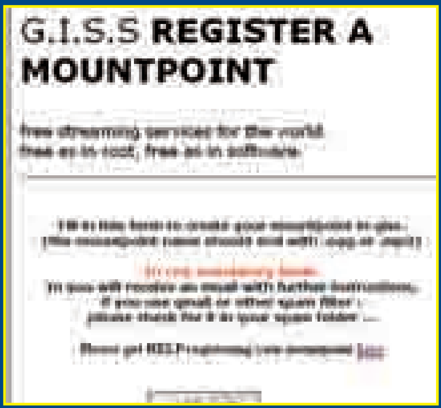
Libertà di parola, libertà di stampa e di informazione: bei concetti che però sempre più spesso devono soccombere alla bramosia di determinate figure che, in alcuni contesti socio-politici, pretendono di avere il controllo su quanto la voce libera delle persone vuole divulgare. Con questo non vogliamo stabilire una volta per tutte chi ha ragione e chi no, si tratta semplicemente di un dato di fatto. In alcune realtà, specialmente in Paesi occidentali o comunque più avanzati, le minoranze riescono lo stesso a far conoscere il proprio pensiero. In altre realtà invece è praticamente impossibile e anche chi svolge mestiere di informazione volesse riportare verità o semplici fatti scomodi per qualcuno, finisce con l'essere censurato. Ecco perché è nato GISS (Global Independent Streaming Support): un sistema basato su libero software e libere infrastrutture per permettere a chiunque voglia far conoscere al mondo situazioni che non troverebbero spazi nell'informazione canonica di farlo, disponendo semplicemente di una connessione a Internet e di un computer dotato di microfono o di webcam.

:: La struttura

GISS si basa su una rete di server indipendenti, ognuno collegato agli altri, con cui vengono veicolate le informazioni in tecnologia streaming ai visitatori. La struttura di base è quindi molto semplice: chi ha un server e vuole mettere a disposizione del sistema GISS parte della propria banda e del proprio spazio può farlo implementando in proprio un sistema di streaming audio o video, basato su software libero: esistono numerosi progetti Open Source che offrono questa possibilità e il progetto GISS stesso mette a disposizione un Live CD speciale, basato su Ubuntu, con gli strumenti per creare la propria sorgente di streaming. Da qui, il flusso passa sul server GISS mediante un mountpoint, ovvero un punto di inserimento, per essere reso disponibile a tutto il pubblico. In pratica, il server GISS fa da relay per il nostro streaming. Tutte queste fonti vengono poi indicizzate per contenuti e geograficamente, in modo da renderle più facilmente rintracciabili per il pubblico.

:: Il nostro canale

Per iniziare a trasmettere su GISS abbiamo bisogno di creare un



Il modulo di registrazione da compilare per ottenere un nostro canale GISS.

account sul server principale, all'indirizzo http://giss.tv (è il server che indicizza tutte le sorgenti). Per l'iscrizione dobbiamo decidere a priori come si chiamerà il nostro flusso audio o video: al momento può essere costituito solo da file MP3 oppure OGG, quest'ultimo preferito in quanto completamente Open e in grado di veicolare informazioni sia audio sia video. Facciamo clic su Create your channel per registrare il nostro account: compilato il modulo che ci viene presentato e fatto clic su add mountpoint, riceveremo un'email che ci permette di attivare il nostro account e ci comunica i dati di accesso (che sono il nome del file del nostro flusso streaming e la password generata dal server). In base al sistema operativo installato sul computer che useremo per trasmettere, abbiamo a disposizione diverse scelte software per l'implementazione del flusso multimediale. La scelta va fatta anche in base al tipo di informazione che vogliamo trasmettere. Per un flusso esclusivamente audio, su Linux possiamo scegliere tra MuSE (http://muse.dyne.org), Pure Data con patch OGG o MP3 (http://puredata.info) o Internet DJ Console (http://www.onlymeok.nildram.co.uk) i combinazione con Jack Audio Server (http://jackaudio.org). In ambiente Windows o MacOS X invece possiamo usare al momento solo Pure Data con relativa patch.
Se invece vogliamo trasmettere anche video, in Linux la scelta può cadere su Theora Streaming Studio (http://gollum.artefacte.org/tss), su un semplice script Python che troviamo all'indirizzo http://giss.tv/wiki/images/f/fd/Dvstream.pys (da rinominare in .py e da avviare con python Dvstream.py), su Pure Data con patch GissPdpDv o su DvSwitch (http://dvswitch.alioth.debian.org/wiki). Pure Data è anche l'unica scelta possibile in ambiente MacOS X, mentre Windows dispone di VisionAir (http://dir.visonair.tv/streamer.php), anche se non è pienamente supportato da GISS. Con gli stessi software appena citati è possibile anche trasmettere in streaming video catturato in tempo reale, attraverso una videocamera collegata al PC mediante Firewire oppure via webcam.

:: Configurazione

Il principio di questa configurazione si applica a tutti i sistemi operativi e a tutti i software che possono essere utilizzati per la trasmissione su GISS. All'indirizzo http://giss.tv/wiki/index.php/Streaming_Tools troviamo una guida su come fare: in pratica, ci occorre sapere l'indirizzo del server su cui pubblicare il flusso (che è sempre giss.tv), i dati di accesso (login source e password quella comunicataci al momento della registrazione), il nome del nostro flusso OGG o MP3 e la porta su cui trasmettere, che è sempre 8000.

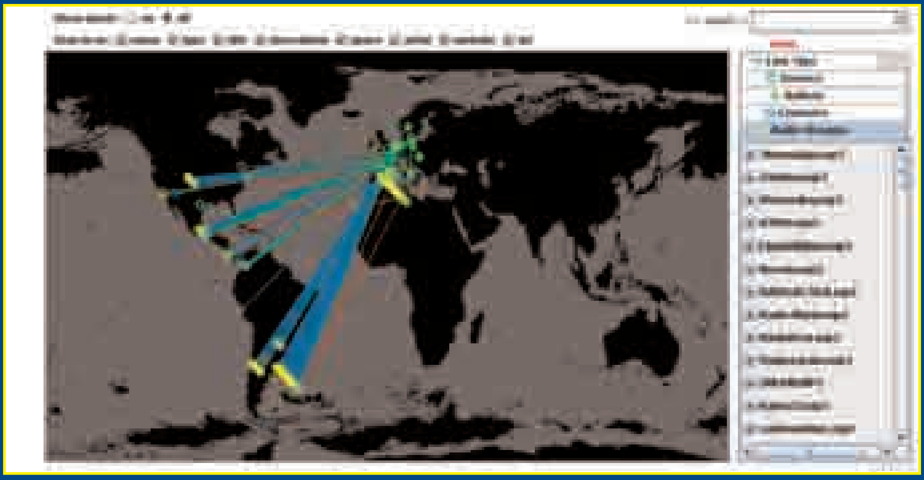
:: In onda!

Quando abbiamo preparato tutto a dovere, possiamo iniziare a trasmettere le informazioni che desideriamo.



La schermata di configurazione di Jack Audio Server su Linux, da usare con IDJC.

Nel pannello di configurazione del nostro canale potremo decidere di renderlo pubblico oppure lasciarlo privato. Ovviamente, è meglio prima fare delle prove in modalità privata e solo quando siamo certi che tutto funzioni a dovere passare in modalità pubblica. Da quel momento il nostro canale verrà elencato tra quelli disponibili a tutti i visitatori del mondo: all'indirizzo http://riereta.net/gisschannel/itheora/index.php troviamo l'indice principale, ascoltabili o visualizzabili mediante il player inserito direttamente nella pagina. In alternativa, è possibile anche cercare canali geograficamente, con la mappa aggiornata in tempo reale che troviamo all'indirizzo http://gollum.artefacte.org/mapuse/map.html.



Con questa mappa possiamo trovare e ascoltare o vedere tutti i canali GISS disponibili.



Da IPv4 a IPv6 (e ritorno?)

Il passaggio dall'utilizzo dalla versione 4 alla versione 6 del protocollo IP è tutt'altro che indolore

Nessuno può obbligare un utente o un amministratore di rete ad aggiornarsi e passare a IPv6: sarebbe contrario alle regole alla base di Internet. Senza contare che questo passaggio può essere piuttosto costoso nel caso in cui l'hardware non possa essere aggiornato ma debba essere sostituito. Allo stesso tempo non è pensabile di imporre una data di cessazione per l'IPv4: Internet è globale e nessuna autorità potrebbe mai stabilire una data, un orario e costringere tutte le nazioni del mondo ad adeguarsi. Così, la transizione da IPv4 a IPv6 deve obbligatoriamente procedere per gradi, mantenendo i due protocolli interoperabili e cercando di far passare gli utenti allettandoli con i vantaggi di IPv6 e senza obbligarli in alcun modo. Un'operazione estremamente complessa e di lunga durata se si considera che questa convivenza forzata "alla pari" si protrarrà, secondo varie stime, oltre il 2025 e che non stiamo proprio parlando di un aggiornamento di un protocollo esistente ma, in sostanza, di due diversi protocolli. Protocolli che stanno alla base stessa di Internet e la cui ricaduta di funzionalità coinvolge tutti gli altri con modifiche che, in alcuni casi, possono avere una portata imprevista.

:: Fratelli? No, cugini alla lontana.

Il problema, inizialmente, era banale: i 32 bit riservati dall'IPv4 all'indirizzamento erano pochi per il numero di devices e utenti del mondo. Si è pensato, quindi, di passare a un indirizzamento a 128 bit, decisamente più adatto a tracciare le risorse a livello globale. Questo cambio, però, ha costretto a riscrivere il formato dell'header dei pacchetti, creando una incompatibilità che si è ulteriormente complicata quando è stato necessario considerare devices diversi dai classici compu-

PERCHÉ?

La versione 4 del protocollo IP prevede uno spazio di indirizzamento di circa 4 miliardi di indirizzi: 4*109, da 0.0.0.0 a 255.255.255.255. Questa capacità sembrava inizialmente sufficiente per qualsiasi cosa ma considerando la popolazione mondiale e il numero di dispositivi potenzialmente collegabili alla Rete, è facile capire che questa risorsa è in rapidissimo esaurimento. Si decise, così, di pensare una nuova versione di IP, che non soffrisse del problema. Nacque, così il protocollo IPv6, quasi un protocollo differente rispetto a IPv4, a causa delle sue differenze sostanziali. Lo spazio di indirizzamento, con 128 bit dedicati, è la sua caratteristica più appariscente e permette la fornitura di circa 3,4*1038 locazioni.

ter e cercare di migliorare le prestazioni e la flessibilità di IPv4. Il risultato è stato quello di passare da un header IPv4 da 160/192 bit, formato da 13 campi di cui uno opzionale, a un header da 320 bit composto da 8 campi. Alcuni di questi 8 hanno, per di più, un significato diverso da quelli dell'IPv4 e mancano di campi equivalenti nel vecchio protocollo.

Questo impedisce de facto che un pacchetto IPv4 possa essere trasformato in modo banale in un pacchetto IPv6 e viceversa. Una situazione simile a quella di alcune lingue umane che hanno parole non traducibili in altre lingue e viceversa: si può ovviare al problema ma la traduzione è un'approssimazione e richiede più parole. Questa differenza sostanziale impedisce anche che i pacchetti IPv6 possano transitare, in modo automatico, su reti IPv4 e viceversa. Manca una qualsiasi forma di retro compatibilità, un'assenza che impedisce a due risorse IPv6 collegate da un router IPv4 di comunicare tra loro. Se all'interno di una rete totalmente IPv4 oppure totalmente IPv6 non si pongono problemi di alcun genere, l'uso di una struttura mista rende difficoltose le comunicazioni. La soluzione, introdotta in diversi apparati di rete da qualche anno, è quella di trattare contemporaneamente entrambi i tipi di pacchetto, replicando sostanzialmente le funzioni dell'IPv4 per i pacchetti IPv6 attraverso una tecnica di Dual Stack ma con risultati deludenti: perché possa funzionare è necessario che una risorsa sia dotata sia di IPv4 che di IPv6, impedendo di risolvere il problema dell'esaurimento dello spazio IPv4. Così si è cercato di introdurre un meccanismo, chiamato Dual Stack Transition Mechanism, che sfrutta al massimo l'IPv6, riducendo il più possibile l'uso di IPv4. Per farlo, gli indirizzi IPv4 da collegare ai pacchetti IPv6 vengono assegnati dinamicamente, risparmiando l'IPv4 da dannosi assegnamenti statici e permettendo comunque lo sviluppo di IPv6. Questa tecnologia, comunque, non risolve tutti i problemi e introduce nuovi livelli di complessità. Cosa accade, per esempio, durante la risoluzione di un nome di dominio? Un DNS restituisce un indirizzo IPv4 in base alla risoluzione richiesta ma con l'introduzione di IPv6 dovrebbe restituire anche un indirizzo IPv6. Questo comporta uno sdoppiamento degli spazi dei nomi, già introdotto dall'ICANN sui root server il 20 luglio 2004, ma introduce anche un quesito interessante: in che ordine vengono restituiti gli indirizzi? Nel caso il richiedente fosse una risorsa IPv6 sarebbe gradita una ricezione di un indirizzo equivalente. Una informazione inutile alle risorse IPv4 che attenderebbero l'arrivo della risoluzione tradizionale. La mancanza di standard ha fatto si che i DNS Microsoft based restituissero prima l'IPv4 e poi l'IPv6 mentre bind e altri DNS server usano l'ordine inverso.

Il risultato di questi comportamenti fuori standard è che un client può fare una richiesta usando pacchetti IPv4 o IPv6 e ricevendo risposte diverse a seconda della tecnologia usata nel server. Un problema non da poco considerando che alcuni dati potrebbero arrivare in modo parziale. La scelta sull'indirizzo da usare, inoltre, viene lasciata al client, con conseguenti problemi di sicurezza per le risorse server. I



L'header dell'IPv4 risente della sua progettazione vecchia di 20 anni. Includeva persino 8 bit, riutilizzati oggi per il VoIP, per specificare il tipo di servizio, così da permettere ai sistemi di modulare la latenza.



L'header dei pacchetti IPv6 è senz'altro più funzionale e meno teorico. Da notare l'indicazione del payload: se azzerata, per convenzione, si ottiene un pacchetto di dimensione massima: lo Jumbogram.

pacchetti IPv4 e IPv6, per la loro diversità costruttiva, hanno instradamenti che possono essere molto differenti. La stessa risorsa potrebbe vedersi recapitato un pacchetto IPv6 che non è stato filtrato da un vecchio firewall e un pacchetto IPv4 che è arrivato da un diverso gateway. Questo dà ai client la possibilità di scegliersi la strada con cui arrivare a un server: nulla di male per i client comuni ma certo un problema di sicurezza in più pensando che possano esistere client malevoli.

:: Ipotesi di collegamento

Considerando la presenza di due protocolli, si avranno risorse che gestiscono solo IPv4, risorse che gestiscono solo IPv6 e risorse miste, capaci di usare entrambi i protocolli. Allo stesso tempo si potranno avere reti totalmente IPv4, reti totalmente IPv6 oppure reti miste. Le combinazioni migliori possibili sono, ovviamente, quelle di risorse inserite in reti che usano il loro stesso protocollo ma ci sono situazioni ben peggiori che occorre valutare e risolvere prima di un'introduzione massiccia dell'IPv6.

Gli esempi si sprecano: server IPv4 consultati da risorse IPv6, server e client IPv6 che usano un router IPv4, intere reti IPv6 che devono scambiare dati con reti IPv4 oppure, persino, reti composte sia da risorse IPv4 che da risorse IPv6 in cui la semplice identificazione di una risorsa può diventare difficoltosa. Ovviamente, tutti questi casi, come molti altri, sono stati analizzati e vanno considerati con tutte le relative implicazioni: è impossibile pensare di introdurre l'IPv6, ormai una scelta obbligata, se non si rende trasparente e interoperabile con tutto l'hardware e il software IPv4 già esistente. Sono già stati fatti, da privati, alcuni tentativi di creare una Internet separata da quella globale ma hanno avuto risultati disastrosi sia dal punto di vista dell'immagine che da quello economico. Occorre, quindi, che la convivenza tra IPv4 e IPv6 sia la più pacifica possibile e ammetta un interscambio tra i due protocolli allettando aziende ed utenti a una migrazione.

:: Gli ALG

Un meccanismo messo in opera per la convivenza di IPv4 e IPv6 sono i NAT-PT. Simili ai normali NAT usati abitualmente con IPv4, il compito dei NAT-PT è quello di traslare gli indirizzi IPv6 in IPv4 e viceversa, garantendo il corretto funzionamento di sezioni miste delle reti. Per svolgere questa operazione, però, occorre che questi NAT usino gli Application Level Gateway o ALG. Questi gateway, generalmente software inseriti in router e firewall, sono pensati per mettere in comunicazione reti totalmente IPv6 con reti IPv4 e si assumono il carico della traduzione per tutto il traffico in transito. In teoria, il loro compito è quello di aprire i pac-



L'RFC 791 del settembre 1981, consultabile sul sito www.ietf.org, spiegava come doveva funzionare il sistema IPv4.

chetti IPv4 diretti all'interno della rete, sostituire gli indirizzi IPv4 all'interno dell'header e viceversa per il traffico in uscita. Nella realtà, la situazione si complica pensando che alcuni protocolli usati (HTTP, POP ma anche molti usati per videoconferenze, giochi e altro) non utilizzano gli IP solo all'interno degli header ma anche nel payload dei pacchetti.

Questo significa che gli ALG, come tutti gli altri sistemi di comunicazione IPv4/IPv6, sono costretti a guardare anche nei dati trasportati, effettuando le dovute sostituzioni. Proprio per questo motivo si parla di ALG al plurale: ogni protocollo deve avere un proprio ALG che si occupi di tradurlo da IPv4 a IPv6 e viceversa. Questa situazione dà vita a due evidenti problemi: il tempo necessario alla trasformazione risulta elevato e la mancanza di un ALG per un protocollo equivale alla mancanza

GLI INDIRIZZI IPV6

A fronte di indirizzi IPv4 composti da 4 numeri separati da un punto, tipicamente 192.168.1.45 e simili, gli indirizzi IPv6 sono difficoltosi da trattare. Usando una notazione decimale, i 128 bit di un indirizzo IPv6 arrivano a una lunghezza di 39 cifre: un po' troppe da memorizzare. Una soluzione è stata trovata usando una notazione esadecimale che è servita a ridurre le cifre a 32. Un ulteriore passo verso la leggibilità è stato fatto dividendo tramite il simbolo dei due punti ogni blocco da 16 bit ed eliminando l'indicazione "0x" usata per segnalare la notazione esadecimale. Alla fine il risultato ha un formato come il seguente ffff: ffff:ffff:ffff:ffff:ffff:ffff:ffff. Sono, poi, possibili altre semplificazioni. Per esempio si possono omettere eventuali zeri iniziali di ogni blocco, così come possono essere eliminati i blocchi composti solo da zeri (senza eliminare il simbolo dei due punti).


IPv6 Address Added for Root Servers in the Root Zone

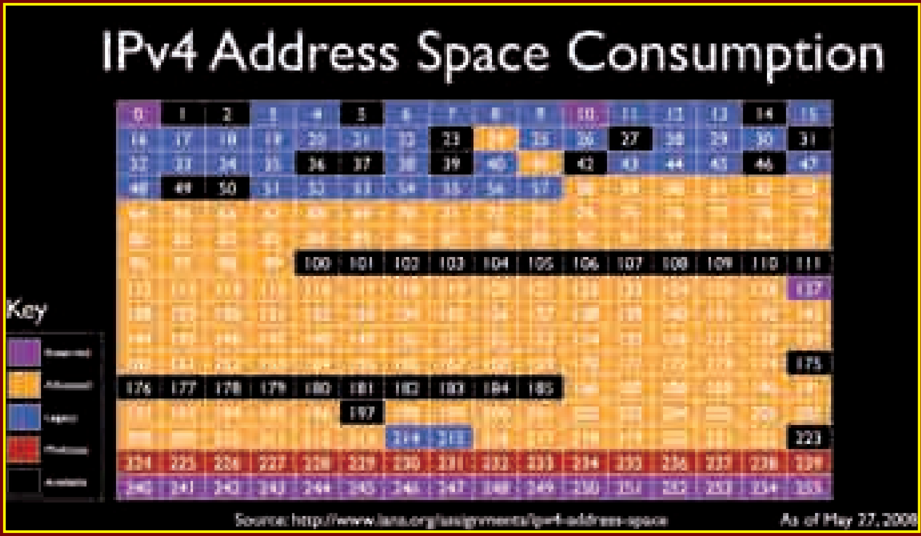
Del 2006 l'annuncio dell'ICANN di aver attivato un servizio DNS IPv6 sui DNS root. Un passo piccolo ma indispensabile per iniziare la trasformazione degli indirizzi da IPv4 a IPv6.

di interoperabilità. Il risultato è che l'uso di ALG, attualmente la strada favorita per l'applicazione massiccia di un IPv6 reale e diffuso, rallenta sensibilmente il flusso di traffico sul network ed ha, come effetto collaterale, l'impossibilità di garantire una copertura di tutte le applicazioni esistenti.

Se alcuni protocolli sono già stati adattati a IPv6, come l'FTP per esempio, altri non lo sono per nulla e gli ALG che dovranno occuparsi di un interfacciamento corretto al 100% sono di là da venire. Basta considerare il traffico gestito da un'apparecchiatura di rete, però, per comprendere subito quante risorse hardware siano necessarie per far funzionare gli ALG e, allo stesso tempo, applicare le funzionalità di NAT-PT, tenendo traccia dell'instradamento dei pacchetti sia IPv4 che IPv6 fino al timeout. Proprio questo è il punto debole irrisolvibile (per ora) dell'intero sistema: in alcuni casi è impossibile aggiornare l'hardware esistente e si è costretti alla sua sostituzione.

:: Tunneling

La comunicazione tra risorse IPv6 tramite reti IPv4 e viceversa viene garantita da tecniche di tunnelling, garantendo i collegamenti point to point tra gli host. L'incapsulamento di pacchetti IPv6 in pacchetti IPv4, per esempio, permette ai nodi IPv6 isolati di poter comunicare facendo transitare pacchetti IPv4 ma senza perdere le caratteristiche dell'IPv6. Una volta raggiunto un nodo IPv6, il pacchetto corrispondente viene de capsulato , acquistando le sue caratteristiche. Più interessante, probabilmente, la tecnica 6to4 che permette a risorse IPv4 di comunicare su reti IPv6 con un tunnelling automatico. Il meccanismo consiste nel generare un indirizzo IPv6 composto da un prefisso riservato ai pacchetti creati con questa tecnica (Hex 2002), l'indirizzo IPv4, l'identificativo della sottorete e l'identificativo dell'interfaccia fisica. Il risultato è quello di permettere il transito di header IPv6 che contengono le informazioni necessarie degli header IPv4. Malgrado la presenza di questi meccanismi, il passaggio a IPv6 sarà lungo e, in alcuni casi, costoso. La stragrande maggioranza dell'hardware di rete installato nel mondo non è di produzione recente e non integra funzionalità IPv6. Allo stesso tempo, l'hardware aggiornabile presuppone l'inserimento massiccio di ALG. Questo comporta un lavoro di programmazione che, se portato avanti in modo impreciso, potrebbe dar vita a ulteriori problemi a cascata. In più, ovviamente, il numero di diversi ALG è destinato ad aumentare esponenzialmente, differenziandosi sia per il protocollo che per produttore, e per modello di hardware. Questo percorso è già iniziato ma il cammino verso l'adozione globale di IPv6 è ancora molto lungo.



Già nel maggio 2008, il numero di IPv4 liberi era in caduta libera. Dopo poco più di un anno è diventato urgente cambiare le cose e impensabile rinunciare all'introduzione di IPv6..

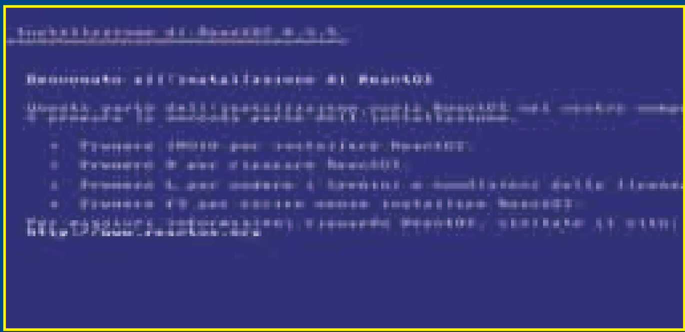
L'ALTERNATIVA OPEN

Windows Open Source? Utopia... Ma qualcosa si sta muovendo, anche se non viene da Microsoft

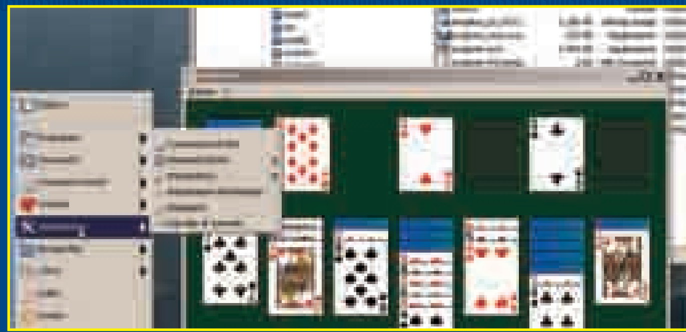
Se ripensiamo a Linux, alla sua storia e alla sua struttura, notiamo che in realtà non è per nulla originale: è un clone, che vede le sue origini in Unix, un clone che ormai è riuscito a soppiantare il modello iniziale. Open è meglio, quindi? Può darsi, a volte sì, a volte è ancora troppo presto per dirlo. Fatto sta che il mercato PC è diviso tra due sistemi operativi, uno chiuso quasi ermeticamente (Windows), l'altro aperto come una finestra in primavera. Però, mentre il primo ancora detiene la maggior parte del mercato, il secondo fatica a decollare come meriterebbe, malgrado sia giunto a un buon livello di maturità, di usabilità e in certi casi abbia perso anche quell'aura da "sistema difficile da capire" che l'ha accompagnato sin dagli inizi. Ora la storia si sta ripetendo, perché anche Windows è in corso di clonazione: non da Wine, che comunque ha bisogno di un altro sistema operativo come nucleo e si limita a essere una piattaforma per l'esecuzione di software scritto per Windows, ma da parte di ReactOS, un'alternativa che si basa su tutt'altra filosofia.

:: Trapianto di core

Non stiamo parlando di un emulatore Windows, ma di un vero e proprio sistema operativo che ha come proprio obiettivo quello di proporre un'alternativa al sistema Microsoft in grado di prendere il meglio da questo. Un'alternativa capace di far girare nativamente la maggior parte dei programmi scritti per Windows e che offra la stessa esperienza d'uso agli utenti provenienti da Windows ma che decidono di tentare la strada dell'Open Source, pur senza saltare sull'altra sponda e passare al Pinguino. Questo è lo spunto che ha spinto alla realizzazione di ReactOS che, pur non essendo ancora un prodotto maturo e pronto per l'uso quotidiano, sta diventando sempre più usabile e compatibile con l'hardware e il software oggi disponibile.
La sua architettura si basa su quella di Windows NT che, al contrario delle versioni 9x e antecedenti, è sufficientemente robusta e performante (malgrado ciò che le malelingue anti Microsoft continuano a dire) per fornire le basi a un buon sistema operativo. Le release oggi disponibili hanno preso spunto da Windows Server 2003 ma non usano nemmeno una riga di codice del prodotto Microsoft: tutto è stato scritto partendo da zero, per non violare alcun brevetto. Questo la dice lunga sulla difficoltà del progetto, che costringe



La procedura di installazione ricorda molto quella delle vecchie versioni di Windows: viene eseguita totalmente in modalità testo e richiede solo pochi passaggi di semplice comprensione.



Il desktop di ReactOS è molto simile (ma non identico) a quello di Windows Server 2003 o di Windows 2000. Allo stesso modo risulta molto simile anche l'aspetto delle applicazioni in esecuzione.

gli sviluppatori a implementare API di sistema il più possibile compatibili con quelle originali senza disporre dei sorgenti di Windows, trattandosi di un prodotto più che blindato. Si è partiti quindi dalla riscrittura del kernel, il nucleo del sistema, per costruirgli quindi intorno tutta la struttura necessaria per il funzionamento ottimale di hardware e software. La principale differenza da Wine consiste proprio nel supporto diretto dell'hardware del PC: ReactOS riscrive anche i driver delle singole periferiche e quindi è in grado di girare come unico sistema operativo del computer.

:: Lo stato attuale

ReactOS, al momento, è rilasciato in versione alpha, quindi è ben lontano dall'essere un prodotto finito e usabile appieno. I problemi cui devono far fronte gli sviluppatori, come già detto, sono numerosi e spesso dovuti alla mancanza di informazioni da parte di Microsoft sui segreti più intimi di Windows. Tuttavia, la release 0.3.9 oggi disponibile (anche se sul sito si parla di una release 3.9.10 in uscita per giugno 2009) è in grado di avviarsi da CD, installarsi su un sistema vuoto e di far girare diversi software scritti per Windows. I driver disponibili, per il momento, non coprono certo tutto l'hardware che possiamo trovare sui computer moderni, però tutto sommato riescono a gestire un PC costruito con componenti standard e sufficientemente diffusi. Possiamo quindi testare facilmente le sue funzionalità, attendendo il momento in cui l'uso quotidiano diventerà possibile. Dal sito Web ufficiale (http://www.reactos.org) possiamo scaricare diverse versioni dell'ultima release disponibile. Sono disponibili l'immagine ISO contenente l'installazione per un computer vuoto e quella che invece offre un'installazione Live, che possiamo quindi provare senza installare alcunché sul nostro computer e senza modificarne la configurazione. ReactOS è in grado di funzionare anche su diverse Virtual Machines, volendo quindi si può tentare anche questa strada: sempre sul sito ufficiale troviamo file già configurati per VMware e per QEMU. Noi l'abbiamo provato con VirtualBox e non ci è parso che si siano verificati problemi particolari, se non quelli dovuti alla lentezza intrinseca delle VM e dello stato embrionale di ReactOS stesso.



Con il Downloader possiamo scaricare e provare applicazioni che già funzionano con ReactOS, posto che il sistema riesca ad andare su Internet.

:: Impressioni d'uso

Pur avendo ben presenti le limitazioni attuali, ReactOS ci è parso usabile e sufficientemente stabile, almeno per quello che riguarda l'interfaccia grafica. Alcuni problemi di refresh delle finestre, specialmente spostandole o sovrapponendole, le abbiamo imputate più al fatto che girava su Virtual Machine che al sistema stesso. L'installazione è rapida e non richiede procedure particolari: si monta l'immagine ISO del CD nel lettore della macchina virtuale, la si avvia e si procede con la formattazione del disco e con l'installazione del sistema senza alcuna difficoltà. Al momento l'unico file system supportato è il FAT, in quanto NTFS non è sufficientemente documentato per poterlo implementare in maniera al 100% compatibile con un sistema Windows reale. Il programma di configurazione non è riuscito a trovare alcuni driver compatibili con la macchina virtuale e quindi li abbiamo saltati, ma dopo il riavvio il sistema era già pronto per l'uso. Alla vista, il desktop di ReactOS somiglia più a un sistema Linux che a Windows, ma provando ad aprire qualche applicazione abbiamo potuto verificare che in effetti la sensazione è quella di usare un sistema operativo Microsoft, dato che anche gli elementi grafici sono molto simili (parliamo però del tema classico di Windows 2000 e non di quello bombato a cui ci ha abituato XP). Tutto sommato è da provare e da tenere d'occhio: non è escluso che un giorno potremo avere a disposizione un'alternativa davvero usabile e soprattutto Open Source per Windows.



Libertà di fare

Impensabile fino a pochi anni fa, ora l'hardware Open è una realtà grazie ad Arduino

Avevamo già parlato, qualche numero fa, di hardware Open: kit elettronici basati su microcontroller che con pochi altri componenti esterni permettono di creare numerose applicazioni pratiche e didattiche. Il principe di questi sistemi è senza ombra di dubbio Arduino (http://arduino.cc), la cui idea iniziale risale al 2005 e che oggi è diventata una piattaforma multiuso semplice, affidabile ed economica per consentire a tutti di sperimentare con il saldatore e i computer. Ma quello che ci inorgoglisce particolarmente è che è un'idea che veste il nostro Tricolore.

:: Un giorno a Ivrea

In realtà il progetto Arduino nasce dalla collaborazione internazionale di cinque loschi figuri: Gianluca Martino, Dave Mellis, David Cuartielles, Tom Igoe e Massimo Banzi, trovatisi in qualche modo coinvolti insieme all'Interaction Design Institute di Ivrea. L'idea di base è la creazione di un modulo hardware facile da costruire e da programmare, collegabile al PC per fornirgli interfacce sensoriali e interattive e che sia indipendente dal sistema operativo usato. Tant'è che l'ambiente di sviluppo per Arduino è implementato in Java, quindi qualunque piattaforma che dispone di tale libreria è in grado potenzialmente di far girare il software. Che quest'ultimo poi sia Open Source non è clamoroso, quanto invece che lo sia tutto il resto: schemi progettuali ed elettrici, documentazione e addirittura il disegno delle PCB, che quindi possono essere liberamente riprodotte in casa, se si è capaci di farlo. Da un'intervista rilasciata da David poi scopriamo che Arduino è prodotto in Italia perché, a conti fatti, disponiamo di impianti più "green" e di costi concorrenziali quanto quelli che farebbe un'azienda cinese, quindi un bel risparmio sulle spese di trasporto.



Il team di Arduino in una rara foto: da sinistra, Gianluca Martino, Dave Mellis, David Cuartielles, Tom Igoe e Massimo Banzi.

:: Che cos'è Arduino

Una scheda Arduino contiene un microcontroller programmabile Atmel (perché economici, versatili e discretamente diffusi) accompagnato da tutta la circuiteria necessaria per interfacciarlo con l'esterno. Acquistando un kit Arduino (sono disponibili anche premontati) troveremo quindi il microprocessore, i componenti elettronici esterni e la scheda PCB per il montaggio, oltre alla documentazione necessaria per l'uso e la programmazione. In genere è tutto ciò che serve per avere un Arduino funzionante: con questo dobbiamo solo decidere come interfacciarlo con l'ambiente, dato che il collegamento con il computer è già previsto via USB, Ethernet o Bluetooth già dalla scheda Arduino stessa. Ma che cosa ce ne facciamo?
I limiti, ed è proprio il caso di dirlo, sono solo quelli della nostra fantasia: possiamo applicare un sensore di luce che, al calare della sera, piloti altre interfacce per l'accensione delle luci del vialetto; collegare un sensore a infrarossi per sapere quando torna a casa il gatto, qualunque cosa. Ci basta sfogliare i molti siti che trattano di elettronica amatoriale, o di hacking in genere, per trovare spunto e progettare un dispositivo tutto nostro basato su Arduino.

:: L'ambiente di sviluppo

Per programmare la nostra scheda Arduino e quindi farle fare ciò per cui l'abbiamo studiata ci occorre l'ambiente di sviluppo disponibile gratuitamente sul sito. Al momento l'ultima release disponibile è la 0016 e la si può trovare anche su Google Code. L'unica installazione necessaria, specialmente in ambiente Windows e MacOS X, è quella dei driver hardware necessari per permettere al PC di comunicare con la scheda: nell'archivio contenente il software è incluso il file readme.txt con tutte le spiegazioni del caso. Chi usa Linux invece è avvantaggiato, perché i moduli per questo sistema operativo sono già compresi negli ultimi kernel. L'interfaccia è molto semplice e intuitiva: i menu e i pulsanti della barra degli strumenti si trovano nella parte alta della schermata, mentre nella parte centrale troviamo le schede dei file aperti contenenti il codice del programma.



Arduino Diecimila, una delle schede disponibili tra i prodotti con interfaccia USB.

Per quanto riguarda il linguaggio di programmazione, Arduino adotta un proprio dialetto basato su Wiring, a sua volta un sottoinsieme del C++. È facile da imparare anche grazie alla presenza di numerose librerie già pronte e dei diversi esempi disponibili nel pacchetto che abbiamo scaricato, quindi se abbiamo già qualche rudimento di programmazione ci basterà aprirne qualcuno per capire la struttura del linguaggio e dei programmi per Arduino.

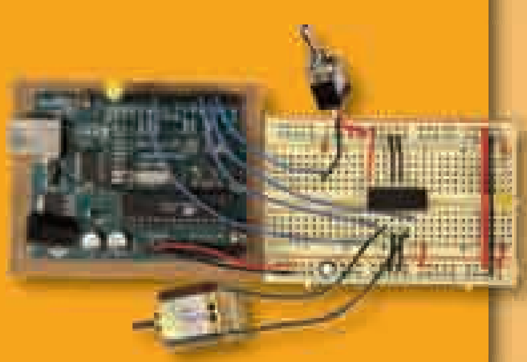
Inoltre, sul sito stesso e su Internet è attiva una folta comunità di hobbysti e di appassionati che scambiano le proprie esperienze e i propri progetti, ed è un punto di partenza quasi obbligato per chi voglia imparare a usare appieno tutte le potenzialità di questo kit.



L'ambiente di sviluppo integrato distribuito con Arduino ci permette di scrivere le applicazioni per i nostri progetti.

:: Già disponibili

Arduino è acquistabile in varie versioni e dimensioni, ognuna con le sue peculiarità: ci sono schede adatte per il principiante che voglia solo sperimentare, come la Serial Single Sided, altre che possono essere impiegate in progetti portatili talmente piccole che possono essere indossate, come la LilyPad, altre ancora di formato standard, come la Duemilanove o la Diecimila. Tutte sono accomunate dal processore che montano e dalla facilità di interconnessione con il PC. I prezzi variano tra i 20 euro delle versioni premontate minimaliste ai 95 euro di quella con modulo Bluetooth, ma volendo si possono acquistare anche solo le PCB e comprare poi a parte i componenti (magari li abbiamo già di recupero), oppure scaricare gli schemi dal sito e costruirci tutto da soli.



Con un minimo di conoscenze di elettronica e di programmazione, si possono creare molti progetti didattici e pratici.

C'ERA UNA VOLTA INTERNET

Leggi cavillose e complesse, ignoranza dei gestori, mancanza di pianificazione e poche oasi felici. Cercare una connessione in vacanza è un incubo.

Avete bisogno di connettervi a Internet in vacanza? Non avete con voi un cellulare con tariffe dati flat o semi-flat? Se fate vacanze in Italia, abbandonate il vostro insano progetto: trovare una connessione può diventare un'impresa disperata. Se all'estero potete trovare una connessione praticamente dovunque, spesso gratuita e aperta a tutti, in Italia non è così scontato.

Eppure, fino all'anno scorso, sembrava che tutti volessero costringerci a collegarci in vacanza: hotel, sale giochi e persino le spiagge disponevano di reti Wi-Fi aperte ai clienti, gratuite o a pagamento, oppure di postazioni fisse da cui collegarsi. Oggi, a causa delle leggi sempre più stringenti sulla necessità di identificare con precisione chiunque si colleghi, riuscire a collegarsi sta diventando sempre più difficile.

:: Patente e libretto, prego.

Proprio le leggi entrate in vigore in questo anno hanno scoraggiato la maggior parte degli esercenti: la mancata o parziale identificazione di un utente comporta per un gestore una multa nell'ordine delle decine di migliaia di euro, con possibile sequestro del locale. Se, prima, una sala giochi non poteva essere completa senza qualche



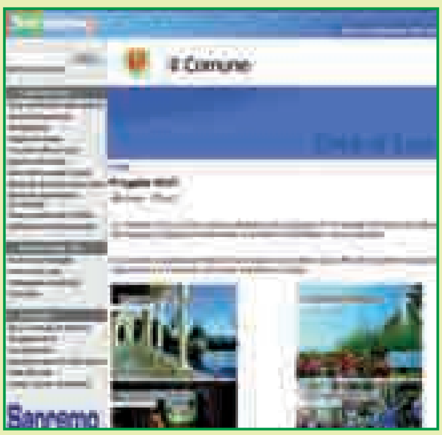


L'installazione de La Fonera, www.fon.com, permetterebbe ai gestori dei locali di fornire un Servizio utile a prezzi accessibili.

postazione dedicata a Internet, lo spauracchio di simili provvedimenti ha decisamente posto un freno al fenomeno, provocando un numero incalcolabile di dietro-front. Atteggiamento favorito anche dal fatto che in un'affollata sala giochi, l'identificazione di un potenziale utente tramite i documenti comporta che questo li fornisca, che se ne possa fare una copia, che vengano custoditi con dovizia dal responsabile e che vengano poi restituiti. In sostanza serve una persona, affidabile e puntigliosa, che si occupi solo di quello. Il risultato, ovviamente, è che unendo il problema legale con la necessità di tenere aggiornati i client, la fornitura di postazioni Internet ai propri clienti diventa economicamente sconveniente: il gioco non vale la candela. Senza contare che potrebbe essere sgradevole, per molti, sentirsi chiedere i documenti da un addetto di una sala giochi. Stesso problema negli hotel: dopo un inizio promettente e favoriti anche dal fatto che l'identificazione degli ospiti è già obbligatoria a causa delle leggi già vigenti, in molti hotel non solo sono sparite le postazioni fisse ma pure gli hot spot presenti fino a poco tempo fa. La causa? La difficoltà di identificare univocamente e in modo sicuro ogni singolo utente. Gli hotel possono facilmente fornire la connessione a un gruppo di persone ben identificate (i suoi ospiti) ma, poi, per l'identificazione di ogni ospite e delle operazioni che ha compiuto, occorrono tecnologie decisamente più costose.

:: Intercosa?

Alla situazione legislativa poco chiara si somma, ovviamente, un'alfabetizzazione informatica più che lacunosa. La maggioranza dei gestori di qualsiasi locale è più a suo agio in cucina, in sala da pranzo o in un ufficio organizzativo. Pensare che si possano occupare di problemi tecnico/legali oltre a un livello basilare oppure che, con la crisi odierna, qualcuno si rivolga a una costosa società esterna per mantenere una infrastruttura adeguata (a sua volta costosa) è una pura utopia. Così, quasi tutti, hanno deciso di rinunciare a fornire questo servizio. Certo, fanno eccezione quegli hotel che dispongono di sistemisti interni (ci sono ma hanno dalle 5 stelle in su) oppure con gestori particolarmente capaci dal punto di vista IT. Per il resto del mondo, l'unica speranza sono i posti telefonici dedicati alle telefonate internazionali, generalmente gestiti da extra comunitari: tariffe abbordabili e buona organizzazione. Peccato che questi siano molto poco diffusi nelle piccole città e anche nelle zone turistiche siano concentrati tutti nelle zone centrali. Il resto è sparito. Proprio per questo motivo i termini del problema cambiano ulteriormente: se, fino all'anno scorso, il mercato non era competitivo perché



Il Comune di San Remo ha in corso un progetto per fornire hot spot. Peccato che sia di utilizzo un po' macchinoso e poco diffuso.



Alcuni hotel hanno un Servizio Wi-Fi e pure ottimo. Un ottimo servizio che, però, è offerto a prezzi di pernottamento elevati.

Internet era disponibile dovunque, a causa della diminuzione di fornitori si riscontra improvvisamente una convenienza a riattivare il servizio. In sostanza: qualunque gestore di locale iniziasse nuovamente a fornire connettività potrebbe ritrovarsi il locale pieno proprio a causa della rinuncia effettuata dai suoi colleghi. Questo ragionamento, per ora, resta sulla carta: tranne che nelle grandi città oppure nelle zone centrali delle città turistiche, riuscire a collegarsi a Internet può diventare un'impresa a cui dedicare ore ed ore.

:: Evvai col Wi-Fi!

Un'impresa che, a volte, diventa paradossale e comica . Basti pensare che in una città turistica come Rimini ci è stato consigliato da più gestori di prendere il portatile e andare alla ricerca di una delle tante reti Wi-Fi casalinghe "aperte". Un consiglio utile, visto che in qualsiasi città basta fare pochi metri con un portatile per trovare tutte le reti che desideriamo. Peccato che sia illegale: connettersi a una rete altrui, se non autorizzati, è un reato gravissimo, anche se questa è aperta e disponibile. Volendo restare nella legalità, noi siamo andati in aeroporto (coperto da un servizio di hot spot) ma non abbiamo potuto fare a meno di notare come una legge sia riuscita a distruggere sia un potenziale plus per i gestori, sia un servizio utile ai cittadini.



vittoria col bot... to

Trucchi e hack pronti a farci diventare campioni con l'MMORPG per eccellenza

Partiamo da un dato: circa 12 milioni di giocatori a pagamento. Questo è il biglietto da visita di World of Warcraft, il gioco di ruolo online (MMORPG) più famoso e di successo della storia, nonché uno dei più affermarti in genere. Come forse sappiamo già, per utilizzare il titolo di Blizzard si deve pagare anche un abbonamento mensile, che parte da circa 11-12 euro al mese. A fronte di questa spesa, abbiamo un mondo virtuale immenso, pronto a ospitare le nostre scorribande fantasy, anche se non è tutto oro quel che luccica. Molte azioni, infatti, sono ripetitive, al punto che per guadagnare oro ed esperienza dobbiamo reiterarle per molto, moltissimo tempo. Insomma, giusto per fare un esempio, per guadagnare esperienza nel combattimento, almeno all'inizio, dobbiamo uccidere decine, se non centinaia, di piccole creature, e questo si traduce in una noia mortale. Insomma, se dobbiamo pagare anche l'abbonamento, tanto vale che siamo liberi di sfruttare il tempo di gioco in un modo migliore, no?

:: Da Lua in poi

Così, qualche hacker con la passione dei videogiochi han pensato di impratichirsi con Lua, linguaggio di script di World of Warcraft, e ricavarne degli interessanti bot. Cos'è un bot? Nella sua essenza è, appunto, uno script, quindi una porzione di codice pronta a eseguire o ripetere automaticamente una determinata azione. Un vantaggio notevole, talmente notevole che Blizzard, produttore del gioco, ha deciso da tempo di correre ai ripari, considerando i bot illegali. In effetti, questi devastano il delicato equilibrio che regna nel mondo di World of Warcraft. Il primo caso ufficiale risale al 2006, quando il colosso americano se la prese con Michael Donnelly, reo di aver creato Glider, un bot specializzato nel gold-farming, cioè la raccolta di oro. Il giocatore pagava Donnelly 25 dollari ed ecco che lui attivava il suo bot. A questo punto, si poteva anche fare a meno di collegarsi al gioco e, dopo qualche giorno, ci si ritrovava (virtualmente) ricchi sfondati. Così è iniziata



Ci sono metodi "automatici" pronti a farci diventare campioni senza alcuna fatica.

la partita a guardia e ladri tra Blizzard e i game-hacker, col continuo rilascio di nuovi script e conseguenti patch correttive pronte a metterli KO. Insomma, ne più ne meno di quanto accade nel mondo della sicurezza informatica!

:: Il potere di Glider

Tra i migliori esponenti del genere bot, ovviamente, c'è proprio Glider, che gode tutt'oggi di buona salute (nel momento in cui scriviamo tutti i i link sono funzionanti, ma potrebbero nel frattempo venire sostituiti, anche se basta una ricerca su Google per sistemare le cose). La disputa legale con Blizzard, in realtà, è ancora in corso, ma una visita su un sito come it.wowglider.eu, ci dà modo di scaricare Glider anche in versione dimostrativa gratuita. L'installazione, da effettuare una volta installlato il gioco e prima di avviare una partita, è tutta automatica. Il costo della versione completa (quella gratuita funziona solo per pochi minuti) è di 29,99 €, ma in cambio otteniamo un bot in grado di effettuare automaticamente un'ampia serie di azioni: gold-farming, pescare, estrarre minerali, lavorare pelli, raccogliere erbe e molto altro ancora. Se invece non vogliamo spendere denaro, e non disdegnano di smanettare con codice e impostazioni avanzate del gioco, uno sguardo su www.mmowned.com/forums/wow-memory-editing/ ci rivelerà hack avanzati che richiedono la modifica dei parametri di memoria. Un semplice esempio? Per muovere il nostro alter ego virtuale in una qualsiasi posizione del mondo di World of Warcraft, è sufficiente modificare con un valore float a 4 byte i seguenti indirizzi di memoria

```
0x0111110C
0x01111110
0x01111114
```

Con, rispettivamente, i valori **X**, **Y** e **Z.** Infine, per confermare l'operazione e dare avvio al movimento, impostiamo a **4** l'indirizzo **0x0111109C.** Sicuramente ci sono modi più semplici e ufficiali di eseguire un'operazione di questo tipo, ma la procedura rivela quanto sia "hackabile" il mondo creato da Blizzard. Ovviamente, per agire al meglio su World of Wacraft e i suoi registri la scelta migliore è il mitico IDA; disassembler molto apprezzato nel campo del "reverse engineering", e che si rivela uno strumento potente e insostituibile nell'analisi di wow.exe, ossia l'eseguibile del gioco Blizzard. Scarichiamo IDA, nella sua vecchia versione freeware, da www.hex-rays.com/idapro/idadownfreeware.htm, mentre la versione più recente è acquistabile da www.hex-rays.com/idapro/.

:: L'ultima novità

Infine, tanto per gradire, è giusto citare anche Mimic, che allo stato attuale appare come il più potente e meglio supportato bot per il gioco di Blizzard. Disponibile anch'esso a pagamento, in una formula ad abbonamento, offre numerosi vantaggi, come un vero e proprio servizio di supporto pronto a contrastare con efficacia le misure anti-cheat messe in atto dal produttore del gioco. Con una spesa di dieci dollari al mese, o 7,99 dollari per circa 200 ore di gioco, Mimic Elite Version consente di ottenere ingenti quantità di oro e mana in modo automatico, senza fatica, e raggiungere alti livelli di esperienza.



La "caccia" a bot e cheat, esplicitamente vietati da Blizzard, si fa ogni giorno sempre più serrata. Ma i game-hacker, per contro, si fanno sempre più furbi ed esperti!

SSL: i server sono sicuri?

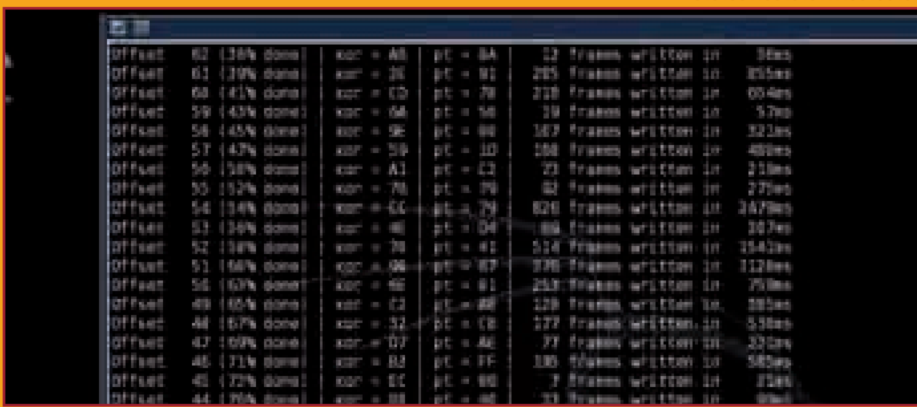


Come funziona la tecnologia SSL e perché non è così sicura come vogliono farci credere

SSL è un protocollo di comunicazione non proprietario nato alla fine del 1994, introdotto da Netscape Communications per proteggere l'integrità dei dati trasmessi tra un server Web e un client e viceversa tramite la reciproca autenticazione tra le parti.

:: Come funziona?

Il principio che sta alla base di SSL è la messa in sicurezza del canale di trasmissione, non direttamente del dato. Proteggere un dato con crittografia e farlo transitare su un canale non sicuro comporta il fatto che prima o poi qualcuno riesca a leggerlo, quindi si è preferito blindare il mezzo trasmissivo, in aggiunta al dato stesso. Quando ci colleghiamo a un qualsiasi sito, il nostro computer si serve di un browser per mettersi in contatto con un server Web che ospita un URL sicuro. Il server Web risponde al client inviando il certificato digitale per l'autenticazione al browser Web. Il client verifica che questo certificato sia valido, non scaduto e soprattutto che sia corretto. Se la verifica va a buon fine, il client genera una chiave, valida solo per quella sessione, per la cifratura di tutti i dati che transiteranno da e verso quel server Web specifico. Per garantire che i dati non siano letti da nessun altro, il client cifra la chiave di sessione utilizzando la chiave pubblica del server Web, contenuta all'interno del certificato digitale. Quel server, quindi, sarà l'unico a poter leggere le comunicazioni cifrate con il nostro client e potrà farlo esclusivamente per quella sessione, in quanto la chiave generata non sarà la stessa della sessione successiva. Per questo scopo, generalmente, viene utilizzato il certificato X.509. A questo punto client e server si sono autenticati e "riconosciuti", la sessione è sicura e le parti possono iniziare lo scambio dei dati senza la possibilità che qualcuno si intrometta a leggerne il contenuto. Questa fase iniziale di "presentazione" si chiama handshake, letteralmente "stretta di mano". I dati sensibili che transitano sul canale sono protetti tramite cifratura con algoritmi a chiave simmetrica con diversi livelli di sicurez-



SSLStrip è un programma per carpire le chiavi da un server che utilizza il protocollo SSL.

za (come DES, 3DES, IDEA, Blowfish e RC4), o asimmetrica (come la firma digitale, l'RSA), che possono essere cambiati nel corso delle sessioni a seconda dei dati che vengono trattati. La scelta del tipo di algoritmo da utilizzare viene fatta nel corso della negoziazione tra client e server Web. L'utilizzo di questi algoritmi serve a garantire che il dato in arrivo sia integro, che cioè non abbia subito modifiche rispetto a quando è partito dalla fonte.

:: Cifratura e messa in chiaro

Il protocollo SSL costituisce l'interfaccia tra il livello di trasporto e il livello applicazione del TCP/IP. In sostanza prende i dati che arrivano dall'interfaccia e li "blinda" prima che vengano instradati al destinatario attraverso il canale trasmissivo, e viceversa. Non lavora sempre però, entra in gioco solo quando tra le parti è richiesta una comunicazione protetta. Deve essere quindi in grado di cifrare e decifrare le informazioni in arrivo e in uscita ogni volta che viene richiesto.

Mentre l'handshake protocol si occupa della gestione della negoziazione, ossia mette d'accordo le parti sul modo in cui comunicare, la parte che gestisce l'effettiva comunicazione cifrata è il record protocol, che non entra nel merito dei dati che deve trattare ma si preoccupa essenzialmente di cifrarli e rimetterli in chiaro.

Il record protocol prende il messaggio in ingresso, lo frammenta in blocchi di lunghezza prefissata e lo comprime utilizzando l'algoritmo concordato in fase di handshake. La lunghezza originale dei dati in ingresso è stata, ovviamente, modificata e ogni pacchetto contiene, oltre a una parte del messaggio originale, anche altre informazioni quali la lunghezza del pacchetto stesso ed eventuali caratteri di riempimento. In questa fase viene prodotto il MAC (Message Authentication Code), un codice che viene inviato prima del pacchetto a cui fa riferimento e che garantisce provenienza e non contraffazione dei dati che lo seguono. A questo punto avviene l'effettiva cifratura dei pacchetti, utilizzando l'algoritmo prefissato. Utilizzando un algoritmo a chiave simmetrica la chiave per cifratura e decifratura sarà la stessa, indifferentemente da chi sia il destinatario (server o client) e chi il mittente della comunicazione.

:: Il certificato

Per la mutua autenticazione tra le parti, l'elemento fondamentale è il certificato. SSL è un protocollo, in sé non contiene alcun elemento di sicurezza. Il livello di sicurezza dipende dal certificato utilizzato dal server per l'autenticazione. Inizialmente la cifratura dei dati veniva fatta utilizzando una chiave privata a 40 bit, attualmente le più diffuse sul mercato arrivano a 56 bit (raramente 128 bit), ma è stato dimostrato che non garantiscono un elevato grado di sicurezza perché sono facilmente frodabili. È sufficiente mettersi in ascolto e catturare le comunicazioni che intercorrono tra un server Web e i client per un lasso di tempo sufficiente per riuscire a carpire chiavi private con meno di 128 bit. Una volta scoperta, è semplice ingannare i client con un "finto" server che utilizza la stessa chiave di quello originale. In realtà è possibile utilizzare certificati con chiavi più complesse (ne esistono a 256 bit), ma l'impiego comporta il dover affrontare un problema strutturale. Più la chiave è complessa più tempo ci vuole per cifrare e mettere in chiaro i dati. Quindi l'accesso alle pagine Web risulterebbe rallentato, a meno di utilizzare server con hardware più performanti. In altri termini l'uso di chiavi veramente sicure comporta l'utilizzo di macchine più costose, ossia investimenti economici che le aziende il più delle volte preferiscono non adottare. Concludendo, attenzione ai server SSL: non sono sinonimo di garanzia assoluta, potremmo trovarci al cospetto di un millantatore, lucchetto o non lucchetto!



I siti di e-commerce basano la sicurezza su SSL. Il lucchetto indica la cifratura dei dati.

Java Mobile

Accediamo a Internet dal nostro cellulare con programmi Java personalizzati

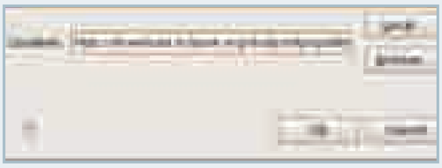


Per tutti i telefonini di ultima generazione la connettività a Internet è un fatto dato assolutamente per scontato. Tuttavia, nella maggior parte dei casi questa possibilità porta con sé effetti collaterali che i produttori di cellulari e i gestori telefonici cercano di non farci notare: ad esempio, diversi telefoni consentono di accedere a Internet solamente tramite poche applicazioni certificate (scordiamoci, quindi, eMule su questi cellulari!); altri, come iPhone, impongono forti limitazioni sullo sviluppo di software personalizzato (ad esempio, il Software Development Kit per iPhone è attualmente disponibile solo per i possessori di un Mac); data la varietà di sistemi a disposizione, è difficile trovare un software che giri su tutti i telefoni; infine, dobbiamo sempre tenere in conto il prezzo da pagare per la quantità di dati che trasferiamo o per il tempo che passiamo collegati a Internet.

Per quanto la tecnologia Java per i cellulari possa ormai apparire obsoleta, essa ci permette di risolvere almeno in parte questi problemi: possiamo infatti creare applicazioni portabili, in grado di girare anche sui telefoni più vecchi e soprattutto progettate ad hoc per le nostre necessità.

:: L'ambiente di sviluppo

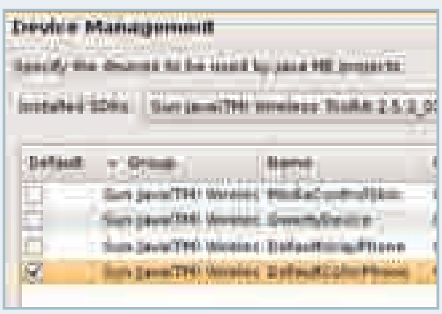
Prima di cominciare a scrivere codice dobbiamo preparare l'ambiente di sviluppo. I software necessari sono l'SDK Java (dalla versione 1.5 in poi), il Wireless Toolkit di Sun ed Eclipse (dalla versione 3.3 in poi) con l'estensione Mobile Tools for Java. Tutti questi programmi possono essere installati sia su una macchina Windows che su una Linux. Il download dei file necessari e l'installazione richiedono un po' di tempo ma non sono particolarmente complicati: i prodotti Sun (Java e il Wireless Toolkit) hanno dei programmi di installazione automatici; Eclipse viene fornito in un file .zip e una volta estratto funziona immediatamente; infine, possiamo scaricare l'estensione MTJ direttamente da Eclipse, aprendo la voce di menu Help->Software Updates, aggiungendo all'interno della scheda Available Software l'indirizzo del repository di MTJ e installando tutti i pacchetti disponibili.



Possiamo installare MTJ direttamente da Eclipse, usando il software di gestione degli aggiornamenti fornito nel download.

:: Ciao mondo

Il nostro primo esperimento non può che essere il classico "Hello World". Il primo passo necessario è creare un nuovo progetto, selezionando in Eclipse il comando File->New->Project, quindi Java ME->MIDLet project. Alla prima esecuzione sarà necessario specificare in quale directory abbiamo installato il Wireless Toolkit di SUN, in modo che Eclipse possa importare da esso i diversi profili di dispositivo per cui possiamo sviluppare software. Per il nostro progetto possiamo quindi scegliere di usare un DefaultColorPhone e fare clic su Finish. A questo punto il nuovo progetto compare nell'albero a sinistra dello schermo. Facciamo clic con il tasto destro sulla cartella src, selezioniamo New->Other e quindi Java ME->Java ME Midlet. Diamo un nome al nostro programma (ad esempio HelloWorld) e facciamo nuovamente clic su Finish: si aprirà automaticamente una finestra contenente lo scheletro della classe Java appena creata. A questo punto dobbiamo completare il codice come descritto in (src/HelloWorld.java), apriamo la scheda Application Descriptor e selezioniamo il comando Launch as emulated Java ME Midlet: se tutto è andato bene dovremmo veder girare la nostra prima applicazione... Ovviamente all'interno del nostro modernissimo telefono cellulare emulato!



Alla creazione del nostro primo progetto dovremo specificare in quale directory è installato il Wireless Toolkit di SUN.

:: Colleghiamoci al Web

Da un semplice Hello World a un'applicazione ben più utile e avanzata il passo è breve: aggiungendo poche righe di codice possiamo infatti far sì che il nostro telefono si colleghi a Internet e mostri il contenuto di un qualsiasi file testuale presente sul Web. Il file completo è disponibile qui (src/WebGet.java). Nonostante questa soluzione sia ancora rudimentale, possiamo comunque intuirne facilmente diverse applicazioni: ad esempio, in qualsiasi momento con il nostro cellulare potremmo controllare lo stato del nostro server, leggere news, controllare la nostra casella di posta e così via.

:: Creiamo pagine ad hoc

La scelta di limitarci a file testuali è dettata solo in parte dalla semplicità: con relativamente poco sforzo e sfruttando la grande quantità di librerie Java a disposizione potremmo interpretare i dati scaricati ed eseguire operazioni decisamente più avanzate su una moltitudine di elementi: testi complessi, immagini e persino video. Una motivazione non meno importante per scegliere i testi puri, tuttavia, è quella del costo dei byte scaricati: a parità di informazioni "interessanti", una pagina Web (magari contenente anche delle immagini) può essere decine o addirittura centinaia di volte più grossa di un semplice testo, il che si traduce in un prezzo più alto da pagare ai gestori telefonici. Naturalmente a loro conviene far credere che una connessione più rapida e costosa sia sempre necessaria, tuttavia noi sappiamo che in molti casi questo non è vero. Possiamo dimostrare questo concetto utilizzando uno script perl (src/treni.pl) creato ad hoc per questo scopo: dati i nomi di due città, esso si collega al sito di Trenitalia, estrae l'orario dei treni che percorrono la tratta specificata e lo stampa in semplice formato testo. Una volta copiato questo script su un server Web, esso è accessibile a tutti e di conseguenza anche all'applicazione Java che gira sul nostro telefono: il risultato è che avremo sempre con noi gli orari aggiornati dei treni, scaricando poche centinaia di byte anziché diverse migliaia, ottenendo le informazioni che ci servono (e solo quelle, senza pubblicità o altri dati superflui) in modo più veloce ed economico.



Hello World, la nostra prima applicazione su cellulare... Per ora solamente emulato!



Poche righe di codice in più, uno script perl che gira su un server e gli orari dei treni arrivano in tempo reale... Quasi gratis!